General Services Administration

Smart Access Common ID Card:
Preliminary Requirements Document

May 10, 1999

Exposure Draft Version 3.0

PREFACE

The Smart Access Common ID Project is a co-operative effort under the leadership of the General Services Administration (GSA) and the Common Access ID Steering Committee composed of representatives from the Federal civilian, defense, and intelligence communities. The project represents a first step in addressing two pressing concerns. First, is the growing concern related to the security and safety of government personnel, buildings, systems, and other facilities; and second, is the need for the Federal government to provide the necessary tools and safeguards to support the burgeoning growth in electronic commerce. A recent Executive Order signed by President Clinton established a joint Government-Industry Presidential Commission on Critical Infrastructure Protection, and CIA Director George Tenet, testifying before the Senate Governmental Affairs Committee, warned that foreign countries have begun to focus on U.S. computer networks for potential cyber-terrorism assaults. In support of electronic commerce, the Government Paperwork Elimination Act of 1998 amended the United States Code to accept electronic signatures to allow electronic submission, maintenance, or disclosure of information to substitute for paper submissions.

The Smart Access Common ID Project utilizes card based technologies, and in particular, smart cards, to provide government employees with a standard identification card that provides the means for employees to authenticate themselves for secure access to government buildings, systems, and facilities. For those employees with heightened security needs, the cards can also carry digital and biometric signatures that may be used for access control and/or electronic commerce.

This document presents the Draft Requirements for a governmentwide Smart Access Common ID Card and the supporting systems necessary to provide secure physical (building) and logical (system) access control and to conduct electronic commerce activities. GSA expects that vendors wishing to support government agencies in deploying the Smart Access Common ID Card and the associated supporting systems will need to develop strategic alliances with other vendors to provide the full range of services required. It is anticipated that the vendor teams will include members conversant in the following disciplines:

- Card platform and database management;
- Physical access control technologies and systems;
- Logical access control technologies and systems;
- Secure provision of Public Key Infrastructure (PKI) services; and
- Biometric technology and services.

Exposure Draft Version 3.0 is directed, in particular, to the vendor community in the interest of obtaining comments on this requirements document and business case considerations. Comments and suggestions should be submitted by June 3, 1999 to:

Larry Carnes
General Services Administration
18th & F Streets, NW, Room G-125
Washington, DC 20405
Phone: (202) 208-7651
Fax: (202) 501-6455
E-mail: larry.carnes@gsa.gov

ACKNOWLEDGEMENTS

The Smart Access Common ID Card Preliminary Requirements Document has been developed under the joint sponsorship of the General Services Administration Office of Governmentwide Policy and the Office of Smart Card Initiatives. The project team wishes to thank the following members of the Common Access ID Steering Committee, who have provided substantial time, effort, and input into this document:

Mike Brooks – General Services Administration
Peter Byrnes – Department of State
Larry Carnes – General Services Administration
Angela Chambers – General Services Administration
Anthony Cieri – Department of the Navy
Brian Clevenger – Social Security Administration
Bill Denk – Social Services Administration
Jeff Dunn – National Security Agency
Mickey Femino – General Services Administration
Keith Gorlen - Department of Health and Human Services
Artch Griffin – General Services Administration
Daryl Hendricks – General Services Administration
Terri Hobson – General Services Administration
Barbara Hoffman – Department of the Navy
William Holcombe – General Services Administration
Craig Howerter – Department of Defense
Mark Krawczewicz – National Security Agency
Robert Maslyn – General Services Administration
Iola Kull – Department of State
Stephen Luther – National Security Agency
Leisa Moniz – Department of Transportation
John Moore - Department of Treasury
Cynthia Musselman – Department of Energy
Marguerite Nealon – Department of the Treasury
Mike Noll – General Services Administration
Fernando Podio – National Institute of Standards and Technology
Jack Publicover – Department of Transportation
Richard Reed – National Security Agency
Lawrence Reiven – National Security Agency
Marion Royal – General Services Administration
Ken Sardegna – General Services Administration
Michael Sulak – Department of State
Dr. Jim Wayman - U.S. National Biometric Test Center
Bill Windsor – General Services Administration

A broad range of Federal agencies were surveyed to obtain requirements for this document. A full listing of agency representatives who completed the survey and participated in interviews is included in Appendix C. Process owners, from Department of Defense and civilian government, provided substantial input to the document, and continue to examine the requirements in the context of this effort. Additionally, members of industry were contacted to obtain information on current technology trends. The project team wishes to thank all of these individuals for their valuable contributions to this project.

TABLE OF CONTENTS

Appendices

Smart Access Common Identification Card
***Draft* Preliminary Requirements Document**

1 INTRODUCTION

1.1 Scope

The Smart Access Common ID Card program will establish a contract vehicle for use by all Federal agencies to acquire a common, interoperable multi-application smart card. This smart card, to be used as an employee identification card, will be acquired from one or more vendor teams, and will be capable of at a minimum providing both physical and logical access control to all Federal agencies. A physical access control system is an automated system that controls an individual's ability to access a physical location such as a building, parking lot, office, or other designated physical space. A logical access control system is an automated system that controls an individual's ability to access one or more computer system resources such as a workstation, network, application, or database. This contract vehicle will provide a menu of products and services that may be accessed by agencies in implementing smart cards for their employees.

The Smart Access Common ID Card is envisioned to be a multi-technology, multi-application smart card that supports several initiatives. These include:

- Heightened government employee security;
- Growth of the Internet and electronic commerce; and
- Continued drive to reengineer processes and enhance services.

The Smart Access Common ID Card will initially focus on providing employee identification and building and computer network access. It will be an Integrated Circuit Chip (ICC) card and will likely include a variety of technologies, among them, magnetic stripe, digitized photo, biometrics, and other media as required by individual agencies. To maximize investments in existing systems, agencies may opt to supplement integrated circuit chip technology with other needed technologies on the card in order to remain backward compatible with their installed legacy systems.

The General Services Administration (GSA) seeks the services of vendor teams to support individual Federal agencies in the implementation of the Smart Access Common ID Card Program. While this program will initially allow agencies to issue an employee card that can be used to provide basic visual identification, identification authentication, as well as physical and logical access control, it is expected that this card will evolve to include additional functionality. Planned functionality for the card includes:

- Identification;
- Building access control;
- Logical access control;

- Digital signature;
- Biometrics; and
- Other value-added services (e.g. rostering, training/certification, property/asset control, electronic forms submission, electronic purse, and medical information).

The agency shall manage the Smart Access Common ID Card and will work with programs to provide cardholder access to services and information for which the cardholder has been authorized or otherwise deemed eligible. The cardholder's digitized color photograph and digitized written signature image may appear on the face of the Smart Access Common ID Card. In addition, the Smart Access Common ID Card shall contain personal information carried on the chip to be used commonly across applications as well as to potentially gain access to other agency facilities. In addition to supplying the card and accompanying applications, the vendor teams may be called upon to provide integration services to allow this card to be integrated with existing or future agency systems.

It is GSA's expectation that in meeting agency requirements for a Smart Access Common ID Card, vendors will provide an integrated card solution. Such a solution must provide not only cards and card management services, but also the full range of functionality addressed in this requirements document. The GSA envisions that vendors will establish strategic alliances among themselves to achieve this "full service" approach that is both interoperable across the Federal community and customized to meet the specific needs and technical environment of each individual agency. It is anticipated that the vendor teams will include members conversant with, at a minimum:

- Card management and customer service provision;
- Physical access control technology and systems;
- Logical access control applications;
- Certificate and Attribute Authority operations and digital signature services; and
- Biometric technology.

1.2 Document Organization

The *Smart Access Common ID Card Common Requirements* document provides an overview of the requirements for a multi-application smart card-based government employee identification card. This document differentiates between those requirements that are considered "mandatory" (likely to be adopted by a majority of agencies) and those that are "optional" (likely to be services customized to the specific needs of a few agencies). The document contains the following sections:

- **Introduction –** Provides an overview of the project and describes the project's scope and objectives;
- **Technical Requirements –** Describes the technical requirements for the components of the card system;

- **Mandatory Functional Requirements –** Presents the mandatory functional requirements of smart card common access ID systems; and
- **Optional Functional Requirements** – Presents the functional requirements for value-added services.

1.3 Objectives

In creating a common identification card for Federal government employees, the three goals of the Smart Access Common ID project are to:

- Develop interoperable application specifications;
- Establish a set of mandatory requirements with optional value-added services; and
- Build in the capability to add new applications and migrate to advanced technologies.

To address the desire of agencies to provide a common, interoperable card that can be used similarly across agencies, this project has defined the following objectives for this card program:

- Interoperability across Federal agencies;
- Open Government System Framework;
- Flexibility; and
- Inter-entity cooperation.

Each of these objectives is described in further detail in the following sections.

1.3.1 Interoperability

Interoperability refers to the cooperative processing of an application by distinct software, hardware/firmware, various generations of cards and terminals, operating procedures, or administrative procedures. In an interoperable environment, there is sufficient flexibility to accommodate cards from multiple issuers, and provide access to multiple services. It ensures that there is flexibility at all levels of service delivery, that investments by consumers and service providers are protected, and that customers have vendor-independent access to services. Interoperability can exist at the following levels in smart cards:

- Physical attributes;
- Electrical attributes;
- Communications protocols;
- Application protocols;
- Application programming interfaces;
- Command and response mechanisms; and
- Secure application modules.

Interoperability, however, entails more than just the technical capability of a card to operate in any terminal. In an environment in which the card is to be used for physical access in non-“home” agencies, the card issuer for the receiving agency may be different from the card issuer for the sending agency. Business agreements must be in place between originating and receiving agencies if the card is to be accepted commonly for physical access across agencies. If the Smart Access Common ID Card includes financial applications, the issue of interoperability may become even more complex. In such an environment, there may be no direct relationship between the card issuer and the acquirer of transactions. To achieve interoperability, both the card issuer and the acquirer must be bound by agreement to a common set of operating rules so that cards bearing the appropriate mark can be accepted at any terminal and the acceptor of the card can be assured of payment in settlement, as well as agreed upon procedures for dispute resolution and liability allocation.

Technical specifications, operating rules, and business arrangements are interrelated in the achievement of interoperability. Technical specifications ensure hardware, software, and data compatibility by configuring system components with each other to pass data and transactions.

While technical standards ensure “physical” compatibility, operating rules provide the management and administrative framework to ensure that transactions are properly handled. The rules define procedures for exception processing and security, and build on technical specifications by defining data flows and procedural standardization. Most importantly, the rules allocate responsibilities and liabilities within the system. Within an open system, operating rules constitute the components of binding business arrangements among the system participants and stakeholders. Currently there are few if any operating agreements across government agencies that address common procedures for card management, as well as intra-agency access to facilities, systems, or data.

Common standards and specifications are imperative to achieving interoperability. Interoperability, in turn, will contribute substantially to the wide-scale acceptance of multi-application cards. Consequently, it is crucial that the issues surrounding standards be resolved if a multi-application environment is to become the norm.

In order to achieve true interoperability in an open system, there is a need to develop sufficient standards and government guidelines to define a multifunctional implementation. The technical standards needed for interoperability exist in ISO 7816 (Contact IC Cards), ISO 10536 (Close Coupling Contactless IC Cards) and ISO 14443 (Remote Coupling Communication Cards). However, the following building blocks must also be in place in order to achieve total seamless interoperability: technical specifications and terminal interface protocols, application specifications, operating specifications, and government business agreements. Because all of these critical building blocks are not currently in place, it is imperative that stakeholders work together to define the standards and government guidelines needed to move toward the interoperability so important to a successful multi-application implementation. The timely development and distribution of specifications, information, and documents will help achieve interoperability at a substantially faster pace.

While there is clearly a risk inherent to moving ahead with multi-application initiatives in an environment in which sufficient standards and government guidelines have yet to be defined, there are some stakeholders who believe that government initiatives in the multi-application environment will result in the creation of de facto standards. It is argued that by having these de facto standards in place, the marketplace will be driven to accept government-defined specifications. In the course of this study, industry has indicated willingness, both in the physical and logical access arenas, to respond to government issued standards or guidelines for products in these areas.

In the absence of the full range of standards needed to achieve seamless interoperability, it may be possible to achieve acceptable levels of interoperability among competing multifunctional card programs. Various pilots have been exploring how to achieve even this limited level of interoperability. One example is the New York City pilot that allows both Visa Cash and Mondex cards to be used in the same terminals by providing multiple Security Access Modules (SAMs) in the terminals. Although this pilot has achieved technical interoperability, management and settlement processes are not integrated, which has resulted in vendors having to perform separate settlement procedures for Visa and Mondex. This pilot has demonstrated the importance of developing both technical and managerial interoperability, even on such a limited scale as these pilot projects.

Initially, this concept of “acceptable levels of interoperability” must be applied to the Smart Access Common ID project. In the early stages of the project, efforts to accomplish interoperability across agencies may have to be limited to technical interoperability achieved at the card level. Use of an interoperable employee card to gain universal access across agencies may be impractical in the near future. A key barrier to the implementation of a common identification card across multiple agencies is the presence of incompatible legacy physical and logical access control systems. These legacy systems use a range of technologies and proprietary protocols for interacting with the databases that maintain employee privileges and control access to facilities and systems. Until existing proprietary physical access control systems can be modified or replaced, for example, interoperability within the context of a physical access control application may mean little more than the ability to read employee data carried on the card and use such data to populate a visitor log. While the long-term objective of this project is to achieve true interoperability, a more limited approach to interoperability may be needed in the short term. As seamless interoperability is a key requirement of the agencies, the government, through the Smart Access Common ID Card procurement, will look to the vendor community to suggest solutions that are interoperable across vendors.

In the longer term, it will become increasingly possible to achieve more extensive interoperability. While attaining interoperability at the card level is currently a challenge, accomplishing interoperability at the application level is even more complex. However, the emerging Public Key Infrastructure (PKI) may provide a potential mechanism for achieving governmentwide interoperability at the higher application level.

Currently, the existing logical and physical access control systems have responsibility for reading the access card, ensuring the identity of the cardholder, validating the status of the card, checking for access privileges, and providing or barring access depending on the results of this validation process. While this approach is successful for validating employees in their home agencies, it cannot accommodate employees seeking entrance to another agency's facilities or systems because different agencies' systems employ different technologies and protocols for conducting this validation process. Consequently, agencies have adopted various incompatible approaches to authenticating identity, managing access privileges, and granting access to visiting government employees.

To address the complexities of achieving interoperability across incompatible physical and logical access control systems, theoretically one could use the emerging Public Key Infrastructure as a mechanism for verifying the identity of the cardholder and the validity of the card. This approach assumes a governmentwide access card that can be read interoperably by card readers at different agencies, as well as the infrastructure to validate the status of digital certificates carried on the card. The Federal PKI Steering Committee is currently working on putting this infrastructure in place and has begun the effort to establish a Bridge Certificate Authority (for definition of this and other related terms, see the Glossary in Appendix A) to enable agencies using different Certificate Authorities (CA) to interoperably exchange certificates. The viability of this approach will depend upon the mix of applications selected by individual agencies and their unique security requirements. For agencies requiring high security, a digital certificate (or an attribute certificate carrying a biometric template) could be used as the basis for employee identification and authentication. A reader at Agency B's facility could read a card carrying a digital or attribute certificate for an employee from Agency A. A standardized application could be used to retrieve the certificate and pass the certificate to the Certificate Authority (CA) for Agency B. Agency B's CA, in turn, could pass the certificate on to Agency A's CA through a Bridge Certificate Authority. Agency A's issuing CA would be responsible for validating the certificate and sending an approval/denial message to the initiating access control application through an appropriate Application Programming Interface (API). The access control application can then securely grant or deny access based on the results of the validation process. Thus, employees visiting agencies could be validated and granted secure access without having to be included in the visited agency's access control database.

An alternative for agencies with lower level security needs is to check only for the presence of a certificate signed by a trusted CA, without validating the certificate status through the Bridge Certificate Authority. This approach is less complex and less costly. It would not depend upon a Bridge Certificate Authority being in place. Thus, the level of security required by an agency, as well as available resources, will dictate the corresponding solution and degree of interoperability acceptable to the agency.

1.3.2 Open Government System Framework

It is the government's objective to develop the Smart Access Common ID Card within an open government system framework to achieve government control and vendor independence, and to encourage competition. In the current smart card industry, card terminal vendors have not yet agreed on a common standard interface. There are similarly numerous competing companies offering various different card operating systems and APIs. This results in a wide variety of commands and response codes. Additionally, card issuers, who may decide where to place card-resident applications on the cards they issue to customers, may place applications and data in very different locations on the card. With potentially multiple vendors supported on a GSA schedule or other government contract mechanism, and highly divergent agency needs, card interoperability and successful integration of card-based legacy applications could well suffer in the current environment.

The smart card industry has embraced a number of initiatives to enhance system openness. These efforts have achieved vendor independence, increased markets, reduced application development times and cost, and improved competitiveness. One example of these initiatives is the development of the Open Card Framework (OCF) by the Open Card Consortium. OCF was developed to address the objectives of smart card terminal vendor independence, smart card operating system provider independence, and smart card issuer independence. As an example of this trend to open systems, this architecture provides the following layers to achieve an open card environment:

- **Card Terminal Layer –** The Card Terminal Layer provides access to physical card terminals and inserted smart cards for which appropriate OCF compliant drivers are made available by a number of manufacturers. This layer solves the problems of card terminal vendor dependency.

- **Card Service Layer –** The Card Service layer makes it possible for OCF compliant cards to deal with a wide variety of card operating systems in existence and the various different functions they may offer. This layer solves the problem of card operating system dependency.

- **Application Management Component –** This component attacks the problem of where applications and data are physically located on the card. This component is capable of locating and selecting card-resident applications on any given smart card, listing the applications that a particular smart card supports, and activating/deactivating applications on the card. This component solves the problem of card issuer dependency.[1]

The layered architecture approach of the *Government Smart Card Technical Interoperability Guidelines* is yet another example of this trend to open systems. Mandating an open configuration that allows government control, vendor independence, and the ability to easily transition to new and emerging technologies in the future, is a key objective of GSA. Therefore, compliance with open frameworks including OCF for smart cards, Open Database Connectivity (ODBC) for databases, generic APIs for biometrics, open operating systems such as Java based systems, and other industry initiatives to achieve openness in system architecture, open source code, and platform transparency for application developers is a critical enabling strategy for this effort.

[1] IBM, OpenCardFramework, General Information Web Document, October, 1998, p. 3-4.

1.3.3 Flexibility

Across the government there is a spectrum of agency security characteristics. Some agencies, including those that comprise the intelligence community, have far more intensive security needs. Agencies with high-end security needs, for example, must have the capability to exchange clearance information with related agencies, protect access to classified information and Sensitive Compartmentalized Information Facility (SCIF) facilities, and more securely authenticate a person's identity. Computer security and network access requirements are also more intensive. Civilian agencies, with different security requirements, will have less need (not "no need") to implement an intensive access control program.

Within all security systems, secure access must be based on the ability to authenticate an individual's identity. As the value of the protecting information/facilities or the consequences of compromising the information/facilities increases, so must the layers of security provided to control access. Consequently, agencies with higher security needs are more likely to implement additional layers of security.

Closely related to these varying levels of need are the corresponding levels of resource availability. Agencies have different priorities and, therefore, different levels of commitment to implementing security improvements. Some agencies are far more willing and able than others to expend the resources needed to upgrade their security systems.

Agencies also vary substantially in their existing security environment. Some agencies have already implemented physical and/or logical access control systems. In agencies in which substantial investment already exists in such physical or logical access control systems, it may be necessary to provide backward compatibility with these legacy systems. The need to support backward compatibility may require the use of multiple technologies on a smart card to provide a migration path from legacy to newly emerging technology.

The GSA understands that agency characteristics and needs diverge. It is the intent of the Smart Access Common ID project to respect agency diversity and encourage solutions that are customized to meet the needs of specific circumstances. While GSA encourages adherence to recognized industry standards and actively promotes efforts to achieve interoperability, the agency's intended role is not to mandate "one size fits all" solutions. Rather, through the concept of "mandatory" and "value-added" requirements, GSA is striving to achieve maximum flexibility by providing the appropriate building blocks to assemble smart card solutions that work effectively to meet the needs of individual agencies.

While some agencies will need merely card enhancements or services to integrate upgraded cards with existing applications, other agencies may need a full menu of applications. Some agencies may elect to migrate their existing systems to incorporate these emerging technologies, while others will have the ability to move directly from legacy systems to emerging technologies, thereby simplifying the process of adopting technology enhancements. The approach of the Smart Access Common ID program is to emphasize flexibility while accelerating the adoption of smart cards across the Federal community. By providing a wide range of products and services from which agencies may select appropriate options, GSA wants to encourage agencies to build smart card-based employee identification and authentication systems that support their mission, enhance their organizational culture, and meet their resource requirements. Consequently, GSA seeks to provide a multi-faceted approach that at once allows flexibility, yet through adherence to common specifications, makes accelerated progress toward interoperability.

1.3.4 Intra-Agency Cooperation

Another concern that will impact the success of an employee card platform is the ability to develop the necessary management structure to achieve a multi-application card platform. It will be necessary to rethink the traditional strategies for card issuance and management. A new paradigm for distributing cards to the cardholder population may have to evolve to address the complex structure needed to accommodate multiple functionality on the card.

The card issuance function may no longer be performed only by the traditional badge issuance entity. As enrollment may entail increasingly complex functionality, such as key/certificate generation and biometric template creation, the card issuance and personalization functions might be managed by public and private entities providing different aspects of card related services. While government entities may provide personnel and identity proofing information, for example, private vendors may be called upon to generate and maintain public key and attribute certificates. Employees may be directed to multiple offices to activate different card applications or privileges (e.g., facility office to be placed in the physical access control database or the computer security office to obtain system authorizations on the card or a new/reorganized office). The smart card management structure may vary from agency to agency. Intra-office cooperation as well as ongoing interaction with private entities will become critical to the smooth operation of a multi-application smart card issuance process. Thus, the GSA contract vehicle must be flexible enough to accommodate divergent approaches to card issuance and management.

1.4 Mandatory and Optional Bid Requirements

To successfully achieve the objectives of an interoperable, open, yet flexible platform, GSA envisions that vendors will provide, and agencies will avail themselves of a variety of card implementation strategies. While GSA wishes to maximize an individual agency’s ability to customize its employee access card implementation, it also is concerned with achieving economies of scale across the government. Consequently, GSA has turned to the concept of “mandatory” and “optional” bid requirements to balance these potentially conflicting aims.

Mandatory bid requirements are those requirements that are presumably shared by a majority of agencies. The Vendor Team(s) responding to the Smart Access Common ID RFP will be required to provide products and services to address all mandatory bid requirements, at a pricing structure that is based upon presumed substantial utilization rates. Although agencies will *not* be required to adopt mandatory functionality, it is assumed that requirements will not be designated as mandatory unless a number of agencies have indicated an interest in the capability. Because it is presupposed that a majority of agencies will opt to use mandatory functionality, they are likely to realize economies of scale when implementing mandatory functions. By designating a capability as mandatory, GSA is, in essence, indicating to the vendor community that there is a high-level of agency interest in that mandatory bid requirement. Vendors, in turn, may reasonably presume a strong market for the capacity in determining their price structure.

At agency discretion, additional options and capabilities may be required for their individual Smart Access Common ID platforms. The need for such options and capabilities may be shared only by a few other agencies. While the Vendor Team(s) will be required to provide all mandatory bid requirements, they will have the authority to decide whether or not to provide optional bid requirements. In developing a pricing structure for optional bid requirements, vendors are likely to assume a smaller market and price the capability at a higher price to compensate for this lower level of interest. Agencies that choose to obtain the optional capability because they have a specific need for it are likely to accept the higher pricing structure. Agencies are therefore less likely to realize economies of scale when they select optional bid requirements.

GSA fully understands that each agency confronts unique circumstances and supports diverse technical and organizational environments. Because of this diversity, GSA realizes that mandating a standard platform is unrealistic. Consequently, GSA seeks to provide a menu of products and services from which agencies can assemble a Smart Access Common ID platform that can operate across agencies, yet meet the unique needs of each agency. The tradeoffs that may need to be made between flexibility and interoperability are likely to affect the ultimate configuration of an agency's card platform. To some agencies, interoperability may be critical, so they will seek to adhere as closely as possible to a "standard" platform. Other agencies may view interoperability as less important, and may assemble a highly individualized platform that is less likely to function seamlessly with other card platforms. Thus, some agencies may elect to build their platform from standard components based predominantly on mandatory bid requirements, while other agencies may concentrate on assembling optional capabilities.

To assist those agencies for which interoperability across the government is a high priority, GSA recommends a set of "standardized" card configurations that utilize prescribed components based on the level of security required. Although the Federal government recognizes a number of security levels, for the purposes of the Smart Access Common ID procurement, GSA suggests the following standard card platforms:

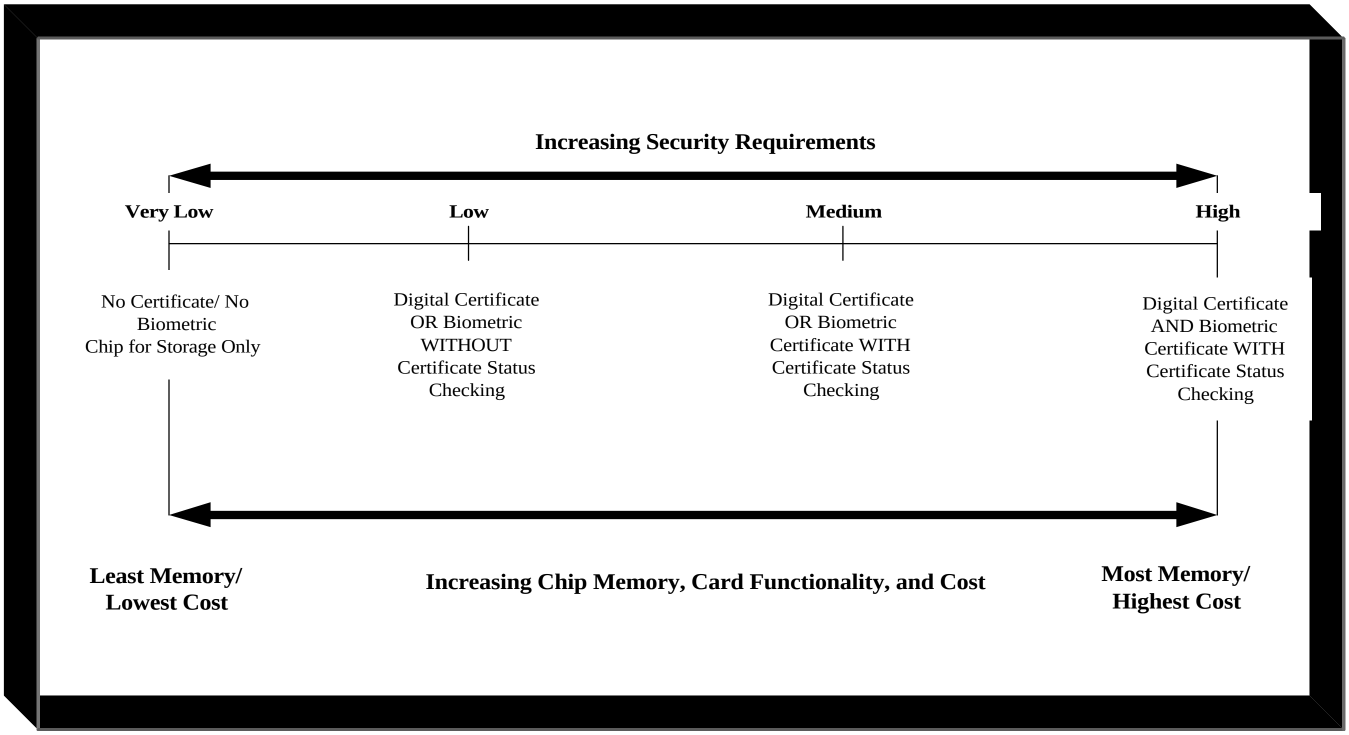
- **High-Security Level –** This platform typically would include both a biometric and a digital certificate capability. Either the biometric or the digital certificate or both (i.e., layered security) could be used, as described above, to achieve interoperable, governmentwide identity authentication and access control (including both logical and physical access control). This platform would depend upon the PKI infrastructure being in place (including multiple Certification/Attribute Authorities, as well as a Bridge Certificate Authority or a Certificate Arbitrator Module) so that digital or attribute certificates from multiple agencies could routinely be verified on-line. For this high-level of security, biometrics could provide yet another factor of certainty for the identity authentication process. At this level, the attribute certificate would be mandated to securely bind the biometric template to the smart card. The high-security platform would most likely require a "high-end" card with a cryptoprocessor and substantial memory to accommodate multiple certificates. It is envisioned that this platform would include both contact and contactless chip interfaces (i.e., a combi chip would be provided) to support a variety of applications.

- **Medium-Security Level –** This platform typically would include a digital signature/certificate capability or a biometric certificate, but not both. The digital certificate could be used to achieve interoperable, governmentwide identity authentication and access control (including both logical and physical access control). As in the high-security platform, the medium-security platform would depend upon the PKI infrastructure being in place (including multiple Certification Authorities, as well as a Bridge Certificate Authority or Certificate Arbitrator Module) so that digital (or attribute) certificates from multiple agencies could routinely be verified on-line. Although a less complex and expensive platform, this card would still require cryptographic functionality. However, it presumably would require less memory than the "high-end" card because it would support fewer certificates (it would accommodate either a digital certificate or a biometric certificate with a biometric template, but not both).

- **Low-Security Level –** Similar to the medium-security level, this platform typically would include a digital signature/certificate capability but not biometrics. However, rather than use a Bridge Certificate Authority to allow on-line certificate status checking across agencies, it would depend only on checking that a certificate has been signed by a trusted CA. Consequently, it would not depend upon an extensive PKI infrastructure being in place. Alternatively, this lower security level may use a biometrics capability, but one that does not verify the validity of an attribute ("biometric") certificate associated with the biometric template. This platform could utilize a "lower end" card. Although the card would still require a cryptoprocessor for a digital signature capability, it would require less memory as it would not necessarily support multiple certificates.

- **Very Low Security Level –** Agencies with even lower level security needs may opt for lowest cost chip cards with no cryptoprocessor or storage of certificates. Agencies using such cards may be interested only in the contact chip for data storage.

Exhibit 1 shows the continuum from lowest security card to highest security card. As this diagram indicates, the capabilities, storage, and cost of the card/infrastructure are likely to increase in proportion to increasing security requirements. Agencies are free to select from a range of products to best meet their individual needs. Those agencies with lower security requirements or to whom interoperability is not as important may be satisfied with lower end cards. However, a card with the capability to store digital and/or biometric certificates (and the requisite infrastructure to validate these certificates) may be needed to take advantage of the emerging Federal Public Key Infrastructure (FPKI) to achieve governmentwide interoperability.


Increasing Security Requirements
Very Low
Low
Medium
High
No Certificate/ No Biometric Chip for Storage Only
Digital Certificate OR Biometric WITHOUT Certificate Status Checking
Digital Certificate OR Biometric Certificate WITH Certificate Status Checking
Digital Certificate AND Biometric Certificate WITH Certificate Status Checking
Least Memory/ Lowest Cost
Increasing Chip Memory, Card Functionality, and Cost
Most Memory/ Highest Cost

2 TECHNICAL REQUIREMENTS

2.1 Smart Access Common ID Card Platform Architecture

The Smart Access Common ID platform shall be designed as an open architecture solution and shall incorporate existing technology standards as appropriate. The platform must be designed to allow for the timely, economical, and easy addition of new application modules as they are identified by the agencies, without impacting existing functions. The design must be flexible and must not rely on a single component supplier or product in such a way that a necessary change or upgrade to the platform would result in a significant loss of investment, a degradation of performance, or require the support or use of agency resources. The design should incorporate off-the-shelf components whenever feasible so as to reduce risk and investment in new development.

The configuration of the Smart Access Common ID Card System will vary substantially from agency to agency depending upon the card management approach, card personalization and issuance procedures, card capabilities and applications, and technical environment selected by the agency. However, the following generic components shall typically comprise the Smart Access Common ID Card Platform:

- **Cards –** The Smart Access Common ID Cards shall be integrated circuit chip cards that may utilize multiple technologies and have varying capabilities.

- **Central Card Management System**– The Central Card Management system should function as the core of the Smart Access Common ID system, and as such, will require connectivity and interfaces with all other system components. It houses the central cardholder database that supports the capture, storage, retrieval, retention, integrity, and management of data necessary for the issuance, status, replacement, renewal and audit of Smart Access Common ID Cards for each agency.

- **Card Issuance Equipment –** The Card Issuance Equipment includes the computers and peripherals needed to capture the information used to enroll a cardholder, personalize the card, load the card with any necessary certificates, and issue the card to the cardholder. The card issuance equipment typically includes:

  – Enrollment Workstation. The Enrollment workstation is used to capture enrollment information and route it to the Central Card Management System and to the equipment (if not the enrollment workstation itself) actually personalizing and issuing the cards. At agency discretion, attachments to the enrollment workstation may include a video digital camera to capture the cardholder’s digitized photo, a digitized signature capture device, and a biometric capture device. Depending on the procedures for capturing demographic data (e.g., through manual entry or legacy system upload), the enrollment workstation may be used to collect demographic data for card personalization. In some implementations, the biometric data and/or Public Keys captured through the enrollment workstation could be directly routed to the Certificate/Attribute Authority workstation as part of a certificate request.

  – Key Generation Workstation. Although key pairs generally will be generated on-board the ICC card through the use of a cryptoprocessor, some agencies may choose to use a separate workstation to generate keys (i.e., software rather than token generated keys). Once keys have been generated, they are securely transmitted and loaded onto the card at the point of card personalization and issuance.

  – Card Personalization System. The Card Personalization system is used to personalize the card with data, photos, key pairs (if not generated by the card itself), and digital/attribute (i.e., biometric) certificates. Attached to the Card Personalization workstation is a card reader used to load information to the chip on the card and a card printer that is used to print information/photos on the face of the card. In some scenarios, the Card Personalization workstation and Enrollment workstation may be the same device, depending upon whether a centralized (i.e., bulk personalization process) or decentralized process (i.e., on-site issuance) is used for card personalization and issuance.

  – Registration Authority System – In some scenarios, if an agency has a designated Registration Authority, there may be a separate workstation to read public keys from the card (or verify biometric data), document identity proofing, and generate a digital certificate (or attribute certificate) request. In turn, the Registration Authority system may receive signed certificates from the Certificate Authority (or Attribute Authority) and place them on the card. The Registration Authority workstation could be the same as the Enrollment workstation and the Card Personalization system in an on-site card issuance location.

- **Certificate/Attribute Authority System –** The Certificate and/or Attribute Authority System is a trusted computer system that receives certificate requests (that would contain public keys and data or a biometric template) from the entity acting as a Registration Authority, and in turn, signs and issues certificates that are returned to the Registration Authority (or Enrollment Workstation/Card Personalization system) for loading onto cards. The Certificate/Attribute Authorities typically will maintain their own repositories (i.e., Lightweight Directory Access Protocol (LDAP) servers) that are used to publish certificates.

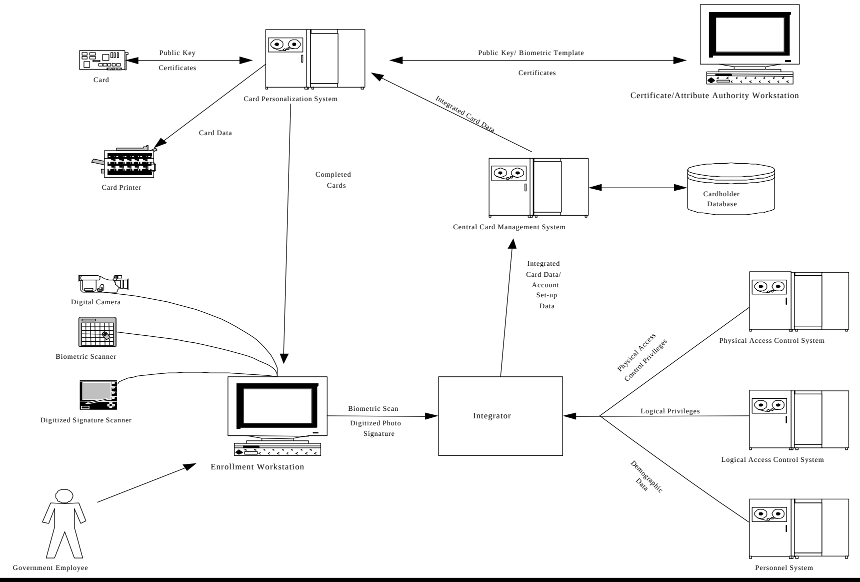
- **Card Acceptance Device** – A Card Acceptance Device is used to communicate with the smart card during a transaction. It is the interface between the card and the application using the card. Card acceptance devices provide power and timing to the ICC and can operate with either contact or contactless interfaces.

- **Applications –** The Smart Access Common ID Card provides access to physical and logical access control applications, as well as to other applications that are a component of the agency's card system. Depending on the card management approach, these applications may communicate with the central card management platform to upload back-up transactions and/or to download hot lists.

- **Interfaces to Legacy Databases –** Many agencies will choose to personalize their Smart Access Common ID Cards with data from existing legacy systems. Thus, important components of the platform architecture are the interfaces from legacy systems to the central cardholder database or to the card issuance workstation.

A sample conceptual architecture is provided in Exhibit 2 below. This diagram is meant only as an example, to illustrate the components of a typical configuration. While the example architecture assumes in-person registration and issuance, bulk personalization, and separate PKI Service Providers (i.e., Certificate Authority and/or Attribute Authority), many other approaches will be used by the agencies, and will affect the overall arrangement of the card platform architecture. In this diagram, an integrator assembles photo, biometric, and digitized signature data from the enrollment workstation, access privileges from the physical and logical access control systems, and demographic data from a legacy personnel database. The integrator aggregates data from these separate systems into a single account-set up file that is sent to the central card management system. This aggregated file is then sent to the bulk card personalization equipment. The card personalization system is able to extract public keys from the card (i.e., key pairs are generated on-board the card prior to distribution), route the keys to the Certificate Authority, and receive certificates to load onto the card. Once the card has been personalized, the completed cards can be sent back to a local office for distribution (or mailed) to employees.

Exhibit 2: Smart Access Common ID Conceptual Architecture


Card
Public Key
Certificates
Card Personalization System
Public Key/ Biometric Template
Certificates
Certificate/Attribute Authority Workstation
Card Data
Integrated Card Data
Card Printer
Completed Cards
Central Card Management System
Cardholder Database
Integrated Card Data/ Account Set-up Data
Digital Camera
Biometric Scanner
Digitized Signature Scanner
Enrollment Workstation
Biometric Scan
Digitized Photo Signature
Integrator
Physical Access Control Privileges
Logical Privileges
Demographic Data
Physical Access Control System
Logical Access Control System
Personnel System
Government Employee

2.2 Smart Access Common ID Card Management System

The agencies shall designate an appropriate entity to produce and issue Smart Access Common ID Cards to designated cardholders on their behalf, and to be responsible for the on-going management of the card base. For each agency, a central card management system that houses the card management database and performs the functions of issuing and replacing Smart Access Common ID Cards shall be required. An agency may elect to manage in-house or outsource its card management system. The system shall include a database management module to support maintenance of cardholder information and card history data. This system shall retain data related to all Smart Access Common ID cardholders and shall provide sufficient back-up and redundancy to ensure the integrity and availability of the data. The card management system shall be available 24 hours per day and seven (7) days per week to accept card status updates and shall be available for on-line functions minimally during agency working hours for the issuance of cards and other normal business functions. This card management system shall be configured so as to provide commercially acceptable response and throughput times for all transactions.

The central card management system shall function as the core of the Smart Access Common ID platform, and as such, will require connectivity and interfaces with all other system components: for the issuance of cards, for the collection of data from legacy systems in support of card issuance, and for reporting of card issuance or status changes to certain other need-to-know card application systems.

All routine systems maintenance and database maintenance shall be performed in a manner that allows maximum flexibility. The central card system must provide 100% functional capability at least 99.5% of the time. The agency designated entity shall be responsible for all aspects of operation, maintenance, upgrades, and modifications of the central card system and must provide adequate staffing with appropriate training to perform the operations and maintenance functions.

The administration of the card management platform may vary by agency. Depending on the applications required on the card, as well as the card issuance strategies, the responsibilities and span of control of the card management platform administrator shall vary. If for example, the agency acts as its own card issuer, as well as its own Certificate Authority and Attribute Authority, it is likely that the agency would also function as the card management administrator. In this scenario, the agency would oversee the agency-wide card management functions, as well as in-house Certificate/Attribute services and physical and logical access control applications. On the other hand, if an agency opted for a range of additional applications, including open financial applications, as well as outside card issuance and Certificate/Attribute Authority services, the card management functions may well involve managing the operations and interaction of a variety of organizations. In this scenario, the card platform administrator may be coordinating the activities of a range of entities outside the agency's control including a financial institution (to provide card issuance and/or financial applications), a Certificate Authority (to provide PKI services), an Attribute Authority (to provide biometric verification services), and separate vendors for individual applications residing on the card.

2.2.1 Cardholder Database Management

The database management system shall support the capture, storage, retrieval, retention, integrity, and management of data necessary for the issuance, status, replacement, renewal and audit of Smart Access Common ID Cards for each agency. Sufficient database capacity shall be maintained as the size of the cardholder database increases.

At a minimum, the following cardholder databases shall be required:

- Cardholder basic demographic information;
- Privileges or application inventory of each cardholder;
- Digital signature/public key; and
- Public key certificates.

The maintenance of a back-up database for digitized photos, digitized signatures, and biometric templates shall be at the option of the individual agencies.

The approach used to create the cardholder database shall readily support the capture and linking of data from a number of sources, and the ability to make that data available on a real time basis seven (7) days per week, 24 hours per day. The cardholder database must allow for back up of stored information and easy recovery. In addition, the approach must guarantee the integrity and security of the data. Further, the database solution must be easily extendible to meet the needs of future applications, and be easily accessible to provide for dynamic future reporting requirements. The database must provide a mechanism to audit and track card issuance history and changes in card status, permissions, or demographic information.

For all Smart Access Common ID cardholders, the following data will be stored in the database:

- Unique card serial number;
- Name (first name, middle initial, last name);
- Mailing address, city, state, zip code;
- Agency;
- Office email address;
- Date of issuance;
- Date of expiration;
- Social Security Number/Employee ID Number; and
- Security office number.

At agency discretion, additional data elements may be required. Such optional data elements may include:

- Security clearance expiration date;
- Security access code;
- Residential address, city, state, zip code;
- Gender;
- Department code;
- Office phone/extension number;
- Office FAX number;
- Residential phone number;
- Date of birth;
- Eye color;
- Height;
- Digitized photo image;
- Digitized signature; and
- Other agency specific data.

In support of the digital signature capability, it is expected that an agency designated entity (e.g., Certificate Authority) shall hold the following:

- Digital signature certificate; and
- Public key registration.

In support of the biometric capability, it is expected that an agency designated entity (e.g., Attribute Authority) shall hold the following:

- Attribute certificate with biometric template.

As other capabilities are added to the card, the database management requirements will expand. At a minimum, for each functional capability addressed by this card platform, it is expected that an access key specific to the application will be carried on the card, and will be stored on the central card system to support the card replacement function. Additional application data may be carried on the card and stored in the central card system.

The agency designated entity shall be responsible for the security of the demographic data stored in the cardholder databases and must adhere to Federal privacy laws and regulations.

2.3 Card

The Smart Access Common ID Card will contain the mandatory requirement information as specified in section 2.1.1. The vendor shall provide card design and production services. The vendor shall conform to card specifications indicated as applicable by the procuring government agency that are contained in the *Government Smart Card Technical Interoperability Guidelines*.[2] The card design must be capable of accommodating the selective and economical addition of future applications while minimizing the need to re-issue the card base.

The Smart Access Common ID Card shall be a multi-technology card with the following features[3]:

- An integrated circuit chip with cryptographic capability (if agencies choose to implement digital signature) to support digital signature and public key technologies;
- A contact chip interface to support multiple public sector applications; and
- A contactless chip interface to support physical access control and other high speed transaction applications.

The card shall be made of durable materials. The specifications for the construction and materials to be used in manufacturing the card shall conform to the *Government Smart Card Technical Interoperability Guidelines*[4]. Materials and production processes shall be selected to extend card life. The expected card life shall conform to the specifications in the *Government Smart Card Technical Interoperability Guidelines.*

2.3.1 Physical Characteristics

The Smart Access Common ID Card shall conform to the physical characteristics required in Chapter 8 of the *Government Smart Card Technical Operability Guidelines*[5]. This document addresses card dimensions, construction, card materials, card characteristics, flammability, resistance to chemicals, reliability/durability, and environmental conditions.

[2] U.S. General Services Administration, GSA Smart Card Initiatives, *Government Smart Card Technical Interoperability Guidelines: A Component of the Management Package for Government Smart Cards,* Version 1.0, July 15, 1998, p. 52.

[3] The Smart Access Common ID Card may also include other technologies such as magnetic stripe, bar code, proximity, Wiegand, and RFID for reasons of backward compatibility and to support financial applications.

[4] Ibid., p. 52.

[5] Ibid., p. 52-60.

Physical card security features are designed to deter counterfeiting and/or lifting of data from the magnetic stripe, employee picture, bar code or chip. The card shall be made of tamper resistant materials such that any attempt to alter or reuse the card shall be apparent to the naked eye. The card design shall embody security features to include full color printing, a hologram, ultra violet ink, fine line printing, shadow photo and/or other features that protect against counterfeiting.

2.3.2 Card Standards

There are a number of standards affecting both the physical appearance and the technical requirements of cards. These standards are discussed in the sections below.

2.3.2.1 Physical Standards

The Smart Access Common ID Card shall conform to smart card standards developed by the International Standards Organization (ISO). Specific standards include:

- ISO 7810 Identification cards – physical characteristics;
- ISO 7811 Identification cards – recording techniques;
- ISO 7813 Identification cards – financial transaction card;
- ISO 7816 Physical characteristics of integrated circuit cards with contacts; and
- ISO 14443 (currently in Draft status) Contactless integrated circuit card – remote coupling cards.

In adhering to ISO standards, the Contractor shall be required to comply with any revisions to the current standards.

2.3.2.2 AAMVA Imaging Standards

The Smart Access Common ID Card shall comply with the following American Association of Motor Vehicle Administrators Best Practices guidelines:

- *Best Practices for Digital Image & Signatures;*[6] and
- *Best Practices for Bar Code, if bar code is specified as a required feature under the Statement of Work.*

2.3.2.3 Data Storage Standards

Although there is currently no formally accepted standard for storing digital credentials (i.e., keys, certificates, etc.) and other data on smart cards, there is a recommended approach that is in the process of being adopted as a standard. The Smart Access Common ID Card shall comply with the following working public draft:

- RSA Laboratories PKCS #15 V.1.0: Cryptographic Token Information Format Standard.

[6] *Best Practices Imaging Standard for Photographs and Signatures*, Prepared by the Digital Imaging Standards Subcommittee, November 1994.

2.3.3 Mandatory Card Technologies

The Smart Access Common ID Card shall be based on integrated circuit chip technology. The card shall incorporate both a contact and contactless interface. The card may optionally be a hybrid card with contact and contactless chip interfaces linked to separate processors, or a combi-card with contact and contactless chip interfaces sharing a common processor.

2.3.3.1 Integrated Circuit Chip

The Smart Access Common ID Card shall include an integrated circuit chip. The initial applications that will reside on the chip shall be the demographic data, digital certificates, and biometric templates (contained within attribute certificates) to be used for identification authentication, physical access, and logical access control applications. Over time other public sector applications will be added to the Smart Access Common ID Card. To ensure adequate capacity for applications, the Federal agency shall determine its strategy for sizing the chip and for allocation of chip space across different agency applications.

The integrated circuit chip shall have the ability to perform cryptographic functions. This capability typically shall be provided by a cryptoprocessor.

2.3.3.1.1 Contact Interface

The contact interface shall be used for employee identification authentication and logical access control applications, and optionally for physical access control and any other data storage and retrieval applications required on the card. The contact chip location and dimensions, contact assignment, and card session shall be in compliance with Section 8.5 of the *Government Smart Card Technical Interoperability Guidelines*[7], as well as the following integrated circuit chip standards:

- ISO 7816-1: Identification Cards-Integrated Circuit(s) with Contacts – Part 1: Physical characteristics;
- ISO 7816-2: Identification Cards-Integrated Circuit(s) with Contacts – Part 2: Dimensions and location of the Contacts;
- ISO 7816-3: Identification Cards-Integrated Circuit(s) with Contacts – Part 3: Electronic Signals and Transmission Protocols; and
- ISO 7816-4: Identification Cards-Integrated Circuit(s) with Contacts – Part 4: Interindustry Commands for Interchange. (The agencies should agree upon the options to exercise within this standard to ensure interoperability).
- ISO 7816-5: Identification Cards-Integrated Circuit(s) with Contacts – Part 5: Number System and Registration Procedure for Application Identifiers;
- ISO 7816-6: Identification Cards-Integrated Circuit(s) with Contacts – Part 6: Inter-industry Data Elements;
- ISO 7816-7: Identification Cards-Integrated Circuit(s) with Contacts – Part 7: Interindustry Commands for Structured Card Query Language (SCQL);

[7] *Government Smart Card Technical Interoperability Guidelines*, Op. Cit., p. 59-60.

- ISO 7816-8: Identification Cards-Integrated Circuit(s) with Contacts – Part 8: Security Related Interindustry Commands; and
- ISO 7816-10: Identification Cards-Integrated Circuit(s) with Contacts Part 10: Electronic Signals and Answers to Reset for Synchronous Cards.

2.3.3.1.2 Contactless Interface

The contactless interface shall be optionally used for physical access control. Additionally, the agency may opt for other applications (e.g., transit or electronic purse) that could be implemented with a contactless interface.

The contactless card and reader communicate through RF phase modulation. The contactless card reader radiates its RF energy through a transmitter antenna, the component that determines the effective range of the entire system. The radiated energy of the transmission must increase as the cube of the distance between the card and the reader increases. Thus the signal needs to be 1000 time stronger at a distance of 10 centimeters from the card than at a distance of 1 centimeter.[8]

The most critical component of a contactless reader is the transmitter antenna. Antennas are necessary for proximity readers to send and receive RF signals. The selection of an antenna is determined by the frequency and size of the area to be detected. The card's antenna's frequency and detection range shall be appropriate for the area in which the contactless reader will be installed.[9]

The Contactless chip shall perform in compliance with the following standard:

- ISO 14443 (currently in Draft status) Contactless integrated circuit card – remote coupling cards (Depending on the implementation, the card must adhere either to Type A or Type B standard).

If an agency chooses to use a close coupled contactless card, it shall be in conformance with ISO 10536: Identification cards – Contactless integrated circuit(s) cards.

2.3.3.1.3 Operating System Characteristics

The chip operating system interprets commands sent by the workstation and carries out the requested functions. The commands shall be compliant with ISO/IEC 7816-4. The operating system shall comply with the guidelines set forth in the *Government Smart Card Technical Interoperability Guidelines*[10].

The Chip Operating System (COS) shall be based on emerging open standards and shall support multiple applications, including physical and logical access control, digital signature, biometrics,

[8] 3-G International, *Smart Card Access Control*, p. 29.
[9] Ibid., p. 30.
[10] *Government Smart Card Technical Interoperability Guidelines*, Op. Cit., p. 27.

and potentially other applications. The government discourages the use of proprietary smart card operating systems.

The COS shall be designed to ensure that firewalls are built between applications and that access to each application is restricted to authorized individuals or entities. The COS shall be designed to accommodate the dynamic loading of applications and provide adequate security procedures to ensure the secure loading of such applications. If applications are to be dynamically loaded to the card, the operating system shall be able to verify that the applications being loaded are coming from a verified source. The operating system shall verify the authenticity and integrity of the application to be loaded.

The COS architecture shall include security features that ensure the integrity of the chip applications. Many of the security requirements presented in Sections 5.1.1, 5.1.2, and 5.1.3 should be able to be enforced by the operating system. Furthermore, the COS should support role-based authentication as defined in FIPS 140-1 Level 3.

2.3.4 Optional Card Technologies

In a multi-application environment, some applications may require technologies in addition to the integrated circuit chip. Creating a migration path from existing systems to a multi-appliation smart card technology may necessitate adding technologies to the card. When moving from a single application card to a multi-application smart card environment, existing systems may need to be integrated with the new smart card technology. For example, to provide the capability to achieve backward compatibility with existing physical access control systems, the card should optionally contain other technologies such as magnetic stripe, proximity, Wiegand, RFID, or bar code, depending on the technology used by the installed system. Optional financial applications may also dictate the use of a magnetic stripe.

Such multi-technology cards may take diverse forms including a chip embedded in a proximity or Wiegand card or multiple magnetic stripes appended to the back of a chip card. Although the card at a minimum shall have an integrated circuit chip, the combination of technologies required on the card in addition to the integrated circuit chip shall be determined by the individual needs of each agency.

2.3.4.1 Magnetic Stripe

The Smart Access Common ID Card may optionally have one or more magnetic stripes on the back of the card. According to the *Government Smart Card Technical Interoperability Guidelines*: “The encoding of each magnetic stripe track depends on the application. For example, track 2 is used by the financial community for financial transaction cards in accordance with ISO/IEC 7813 and by the security community to carry security credentials in accordance with SEIWG-012. The encoding used for these two applications is different and therefore will not interoperate.”[11] Consequently, one magnetic stripe may be needed for physical access control systems. A second magnetic stripe may be reserved for on-line financial transaction

[11] Ibid., p. 55.

applications such as commercial debit or credit, if an agency opts to include financial applications on the card.

The agency shall require an approved approach for determining the appropriate time to encode the stripe. When encoded, the encoding shall comply with ISO 7813 Identification cards, financial transaction cards and ISO 7811 – Identification cards, recording techniques. If the agency opts to have financial applications on its Smart Access Common ID Card, it shall need other features, such as a branding logo, a PAN and expiration date on the face of the card, which are required by financial applications.

Agency cards that require the use of magnetic stripe technology must comply with the specifications for magnetic stripe technology contained in Sections 8.25 and 8.3 of the *Government Smart Card Technical Interoperability Guidelines*.[12] Agencies may choose to place information residing on the magnetic stripe on the integrated circuit chip as well.

2.3.4.2 Proximity

The Smart Access Common ID Card shall optionally use proximity technology to provide physical access control capability. The proximity technology uses a contactless interface with a card reader that incorporates an electronic chip and antenna embedded within the card that emits a unique radio frequency signal whenever it comes within range of the electronic field of the reader. The reader distance can vary from several feet to several inches. The Smart Access Common ID Card shall provide the capability to combine integrated circuit chip technology with proximity technology by embedding a chip in a proximity card.

2.3.4.3 Wiegand

The Smart Access Common ID Card shall optionally use Wiegand technology to provide physical access control capability. The Wiegand technology provides a contact interface that must be "swiped" through a slot similar to a magnetic stripe card. The Wiegand card contains a magnetic coating that is embedded inside the card during card production. It provides a more secure and durable capability in abrasive environments. Wiegand readers require less maintenance because of their encapsulated design. Some Wiegand cards have a thickness greater than the specified ISO standards and therefore may not be able to achieve interoperability with other cards.

2.3.4.4 Radio Frequency Identification (RFID)

Radio Frequency Identification (RFID) is used in access control, traffic control, and some specialized industrial control applications. It makes use of a tag, which can have many shapes, including that of a credit card. The tag contains an antenna. When the antenna comes within range of a reader, it generates enough energy to power up a circuit in the tag, and to transmit the identification number contained in the tag. Most RFID tags function like proximity technology in

[12] Ibid., p. 54-55.
[13] Ibid., p. 54-55.

that they are read only. Although RFID and proximity both use radio frequency antennas, they function at different operating frequencies, distances, and voltage.

2.3.4.5 Bar Code

At the discretion of individual agencies, bar code technology may be required on the Smart Access Common ID Card to support backward compatibility with existing legacy systems. Bar code technology typically has been used for such applications as library cards or asset control/inventory management. Bar code technology on the card must comply with the provisions of Section 8.4 of the *Government Smart Card Technical Interoperability Guidelines*.[14]

The required bar code, if two dimensional, shall be in the AAMVA compliant PDF-417 read/write format and included on the bottom right hand corner on the back of the card. It must comply with AAMVA Best Practices for bar codes. Only the application specific information for which the bar code is required shall reside on the bar code.

2.4 Other Mandatory Card Capabilities

The Smart Access Common ID Card shall provide additional technical capabilities to support enhanced cardholder identity authentication and access control. The additional capabilities used to enhance the level of identification authentication provided by the Smart Access Common ID Card may include the following:

- **Biometrics –** The measurement of a unique biological feature used to verify the claimed identity of an individual through automated means. The biological feature may be based on a physiological or behavioral characteristic. The physiological characteristics measure a physical feature such as a fingerprint or face. The behavioral characteristics measure a reaction or response such as a signature or voice pattern.[15]

- **Public Key Cryptography (Digital Signatures/Certificates) –** The use of a cryptographic method that relies on pairs of cryptographic keys, one of which is private and one is public. If encryption is done using the public key, decryption requires application of the corresponding private key and vice versa. Public key cryptosystems make possible authentication schemes in which a secret can be verified without the need to share the secret. Digital signatures are generated with the private key component of the public/private key pair. The corresponding public key is used to verify the signature. Given that a user's private key is never shared with another party, then there can be a strong association between the user's identity and the use of the private key.

The technical requirements for public key infrastructure and biometrics are detailed in this section. The functional requirements for these additional capabilities are presented in Sections 3.5 and 3.6 respectively.

[14] Ibid., p. 55-59.

[15] FIPS Publication 190, Guideline for the Use of Advanced Authentication Technology Alternatives, September, 1994, p. 32.

2.4.1 Biometrics

In the context of the Smart Access Common ID Card program, biometrics shall be used for identification authentication and access control. Biometrics are methods of measuring the inherent physical attributes of an individual. This measurement is usually performed to identify an individual or to verify a claimed identity. Biometrics can be used in two ways: identification and verification. Identification compares a live biometric scan against a database of biometric templates to identify a given individual. Verification entails matching a live biometric scan against a single template carried on a smart card to verify the individual's identity. Verification (matching one to one) typically requires a more simplistic algorithm and performs better than identification (matching one to many). For the purposes of the Smart Access Common ID Card program, the use of biometrics shall be limited to verification (one to one matching).

There are many different biometrics in use today and several others under investigation or development for identification and authentication. Each of these physiological or behavioral characteristics has its own set of strengths and weaknesses. Some are too intrusive to be accepted by the general user population while others may not afford the high degree of accuracy required in some applications.

2.4.1.1 Biometric Selection Considerations

A number of factors must be considered by the agencies in selecting the right approach to use in biometric authentication. The *Guidelines for Placing Biometrics in Smartcards* recommends that: "you must understand the application, the user base, and the characteristics of the biometric device itself. You must also consider the conditions under which it will be used and how fallback authentication methods, such as passwords or tokens, will be instituted when biometrics are not available."[16] When choosing among biometrics, agencies should take into account user, implementation, and product considerations, as recommended in the *Guidelines for Placing Biometrics in Smartcards*.[17]

User considerations include the following:

- **Public Acceptance –** Collection of biometric information may be the subject of privacy concerns among the target audience. Certain biometrics engender a greater perception among the public of privacy invasion than others.

- **User Acceptance –** Both public perception and degree of intrusiveness can impact user acceptance of certain devices. For example, while retinal scans may have greater accuracy than other biometrics, the invasiveness of the capture device has resulted in public reluctance to routinely use this biometric.

[16] National Security Agency, Central Security Service, *Guidelines for Placing Biometrics in Smart Cards*, Version 1.0, September 11, 1998, p. C-2.
[17]Ibid. p. C-2-7.

- **Target Clientele Characteristics –** Some biometric verification products may have better characteristics for a given target audience. For example, race and gender, occupation, age, and color of eyes can affect the error rate and success of certain biometrics.

- **User Difficulties –** Some populations have difficulty using certain biometric capture devices. Difficulties may be based on alignment in the image capture area or characteristics of a given target population.

- **Ease of Use –** The scanning method, false reject rate, and speed of a product can greatly influence user acceptance. Less intrusive biometric systems are more likely to be successful.

The following implementation issues should be considered by the agencies:

- **Enrolled Image Quality –** Enrollment quality is very important to achieve high operational performance. Feedback on poor enrollment quality can be important to a successful implementation. Balancing software enrollment feedback mechanisms with understanding of acceptable quality by the enrollment officer may be important for implementation of a particular biometric.

- **False Acceptance/False Rejection –** The False Acceptance Rate (FAR) is the rate at which an intruder can be recognized as a valid user. The False Reject Rate (FRR) is the rate at which a valid user is rejected by the system. System administrators must balance the false acceptances versus the false rejects to ensure adequate security while remaining cognizant of user convenience.

- **Uniform Testing –** There is a need for a uniform testing approach to ensure that FAR/FRR are calculated uniformly across products so that agencies can use these rates to assist in the selection of products.

- **Circumvention –** Certain biometric systems are more vulnerable to being fooled by a synthetic device. Consequently, liveliness testing can be a desirable feature to help prevent such occurrences.

- **Cost –** The cost of implementing the whole system may profoundly affect an agency's choice of biometric system. While the costs associated with implementing biometric programs generally are falling, the cost of building the infrastructure still is a barrier for many agencies. Emerging developments in this field may continue to have significant impacts on biometric pricing. Consequently, it is important to ensure that modularity at the application interface is in place to allow interchange of commercially developed hardware components, in order to take advantage of product pricing adjustments in the commercial biometrics market.

- **Continuous Verification –** Agencies with higher level security needs may need to opt for biometrics that support continuous verification in a computer security application. Less intrusive biometrics would be better suited to meet this requirement.

- **Template Storage –** The size of a template may be a factor for agencies selecting biometrics. Only certain biometrics have templates small enough to reside on a smart card. Multiple templates may be needed to achieve necessary levels of accuracy, and the amount of storage needed for these multiple templates may influence the viability of card storage and/or processing capabilities.

- **Computer Resources –** The complexity of matching algorithms may vary from product to product. Agencies are more likely to consider those biometrics that have a reasonable performance characteristic using a workstation with a medium range processor.

- **Calibration –** The complexity of the calibration effort needed to support accurate use of a biometric may affect the viability of the biometric for an agency. The frequency and intrusiveness of periodic adjustments needed to ensure correct reading must be considered.

Agencies may have to contemplate the following product considerations when selecting a biometric to use with the Smart Access Common ID Card:

- **Storage Requirements –** In choosing a biometric, agencies shall have to consider the template size and whether multiple templates per user shall be required. The agencies shall have to weigh template size along with the other factors of choosing a biometric when making a decision on which biometric devices to support. Discussion of the template size is presented in the following section.

- **Processing Time –** The processing time required to scan a live image, process the data into a template, and verify the result may vary from product to product. This time component may be used by agencies to differentiate among products. The maximum processing time to scan, process the image, and verify it against a biometric should be one (1) second.

- **Biometric Upgrade/Obsolescence –** The ease with which a given biometric product can be updated or improved over time may impact an agency’s selection. Because biometric products will change over time, automated upgrades such that a new biometric template is created and stored on a smart card during a verification process would be ideal.

2.4.1.2 Template Size

In an environment such as the Smart Access Common ID Card, storage space on the chip is limited, especially when considering that the card is to address requirements for multiple public key certificates, biometric templates (i.e., attribute certificates), and applications. Consequently, the size of the biometric template is a critical characteristic. The size of the user’s biometric template must be small enough to fit into the smart card. The *Guidelines for Placing Biometrics in Smartcards* recommends a size of 512 bytes or less.[18] The Smart Access Common ID Card shall require the size of each biometric template to be 512 bytes or less.

2.4.1.3 Binding the Biometric to the Smart Card – The Biometric Certificate and Associated Infrastructure

A critical requirement for the Smart Access Common ID Card is to provide a secure means to bind the biometric to the smart card and to ensure that the biometric is properly attributed to the correct individual. Although a variety of techniques is possible to create this binding, GSA adheres to the approach presented in the *Guidelines for Placing Biometrics in Smartcards*. This approach advocates placement of authentication information, including the biometric template in an attribute certificate (i.e. the "biometric certificate") that is placed on the Smart Access Common ID Card when the user is enrolled in the system and issued the card.

The biometric certificate can be retrieved by any system component or application to authenticate the user after a mutual authentication protocol has been successfully completed. The system component or application verifies first the signature of the certificate, and then the authentication information via the means specified in the certificate (depending on the type of biometric template contained in the certificate).

2.4.1.3.1 Placing the Biometric Template(s) in an Attribute Certificate

Attributes, defined in X.501, are "information of a particular type." The attribute describes a characteristic of an associated object. X.509 requires that information be placed within an attribute prior to placing it in an attribute certificate. The attribute chosen for the biometric certificate is the Authentication Information attribute, as defined in Appendix D, section 2.3.3 of the *Guidelines for Placing Biometrics in Smartcards.* The Authentication Information attribute has the following qualities:

- Flexible;
- Open;
- Generic;
- Supports different Authentication Information types;
- Supports multiple Authentication Information data within the same attribute;
- Supports unique parameters for each Authentication Information data;
- Expandable for future technology; and
- Supports compatibility determination.

The Authentication Information attribute requires that each supported biometric has a unique object identifier assigned to it. An object identifier can be issued by any ISO certified Registration Authority (ANSI in the U.S.). The object identifier will insure a unique identifier for processing a particular piece of biometric information by the system.

[18] Ibid., p.10.

In addition to the object identifier, the Vendor shall create a document that describes the processing and matching parameters that will be used by the Authentication Information attribute. This will give the system implementors a mapping between the parameters placed in the attribute and the functions that must accompany the processing of the biometric template.

Once the biometric template, or templates is assembled, it must be ASN.1 encoded as an Authentication Information attribute. The ASN.1 Authentication Information attribute definition is found in Appendix D, section 2.3.3 of the *Guidelines for Placing Biometrics in Smartcards.* The Authentication Information attribute is then used as the only attribute with the biometric certificate. The biometric certificate is then ASN.1 encoded per the X.509 Version 3 definition of an attribute certificate.

2.4.1.3.2 The Biometric Certificate Format

The biometric certificate follows the X.509 Version 3 attribute certificate format. The attribute certificate shall conform to the certificate format and size specified by Appendix D of the *Guidelines for Placing Biometrics in Smartcards.*[19] When creating the certificate the following rules will apply:

- The option used for the IssuerName (the GeneralizedName) will be the DirectoryName. The naming convention defined for the Federal Public Key Infrastructure shall be followed.
- The SubjectName will be used opposed to a baseCertificateID. The option used for the SubjectName (the GeneralizedName) will be the DirectoryName. The naming convention specified for the Federal Public Key Infrastructure shall be followed.
- Extensions shall NOT generally be used. Only the Certificate Policy extention may be used if it is deemed appropriate for Biometric Certificates.
- Optional fields (SubjectUniqueIdentifier and IssuerUniqueIdentifier) shall NOT be used.
- The Authentication Information attribute, as defined in Appendix D, section 2.3.3 of the *Guidelines for Placing Biometrics in Smartcards* shall be the only attribute used.

All certificates used on the Smart Access Common ID Card shall be encoded using Packed Encoding Rules (PER Encoding).

The use of the SubjectName as opposed to a baseCertificate ID implies that the certificate is bound to a person, not another public key certificate. That implies that the biometric certificate can be valid after a public key has been revoked. It also implies that the system needs a separate method to revoke biometric certificates.

2.4.1.3.3 Biometric Certificate Confidentiality

The biometric template within the biometric certificate is considered “sensitive information.” The following steps should be taken to insure that this information is only used by valid entities.

[19] Ibid., p. D-4-17.

A mutual authentication protocol, such as described in Appendix B, Section 3.0 of the *Guidelines for Placing Biometrics in Smartcards*, shall be implemented to provide mutual authentication. The Smart Access Common ID Card should not allow any entity to retrieve the information without a successful completion of the mutual authentication protocol.
The system component or application which processes the biometric certificate must destroy its copy of the biometric certificate after it has completed processing.

2.4.1.3.4 Biometric Certificate Processing

An Attribute Authority must be established to support the creation/maintenance of authentication certificates. At an agency's option, the same authority may or may not create both the public key certificate and the attribute certificate. Other system components may have responsibilities for processing the biometric certificate as outlined below.

2.4.1.3.4.1 Biometric Certificate Processing within the Enrollment Station

After the Smart Access Common ID Card has had the Public/Private key pairs initialized the Enrollment Station will be responsible for insuring the following:

- User name information is collected.
- A biometric livescan is taken of the user to be enrolled. The livescan is processed into a biometric template. The biometric template must be placed in the Authentication Information attribute. The Authentication Information attribute can hold multiple biometric templates.
- The Enrollment Station generates and signs a Biometric Certificate Request Message. This Request Message must contain the Distinguished Name of the Enrollment Station, the Distinguished Name of the User, and the Authentication Information attribute created for the User.
- The Enrollment Station sends the Biometric Certificate Request Message to the Attribute Authority for signature.
- The (Attribute Authority) signed biometric certificate is placed in the Smart Access Common ID Card.

2.4.1.3.4.2 Biometric Certificate Processing within the Attribute Authority

The Attribute Authority is, at a minimum, responsible for:

- Processing Biometric Certificate Requests;
- Verifying the signature of the request as having been derived from a valid Enrollment Station;
- Creating a new attribute certificate for the user;
- Placing its Distinguished name in the Issuer field of the biometric certificate;
- Placing the user's Distinguished name in the biometric certificate;
- Signing the biometric certificate;

- Sending the biometric certificate or a failure status back to the Enrollment Station that sent the request; and
- Creating, maintaining, and distributing Hot Lists and/or Compromised Key Lists (CKLs) for the biometric certificate which it maintains.

2.4.1.3.4.3 Biometric Certificate Processing within the System Component or Application

The System Component or Application (the "Host") is responsible for retrieving and utilizing the biometric certificate for user authentication. Once the biometric certificate has been retrieved from the Smart Access Common ID Card, the following steps should be performed to verify the user.

- The host validates the signature on the certificate.
- The host searches the authentication attribute for the identifier of the biometric device it possesses. If a compatible device is not found the user is rejected.
- A livescan of the user is taken. A biometric template is created from the livescan and compared against the template stored within the authentication attribute. The user is accepted or rejected in accordance with the results of the comparison.

2.4.1.3.4.4 Biometric Certificate Processing within the Smart Access Common ID Card

The Smart Access Common ID Card is responsible for storing the biometric certificate and providing confidentiality of the certificate. The card must be capable of verifying the host via the mutual authentication protocol. The Smart Access Common ID Card should not allow any entity to retrieve the information without a successful completion of the mutual authentication protocol.

2.4.1.4 Conformance with a Biometric API

With the rapid pace of change in the biometric field, a critical requirement for the agencies is to be able to maintain flexibility both across vendors and biometric products. Once they have invested in a biometric infrastructure, agencies must be assured that their infrastructure will support technological advances without major new investment. To ensure such flexibility, a biometric independent, multi-level API is needed. API standardization allows application developers to write software once that will work across biometric technologies and across multi-vendor products within a biometric technology with minimal, if any, changes. Multiple levels of API offer flexibility for application level programmers, whether they require low-level control of the biometric processes or wish to program at a higher level of abstraction.

To encourage investment in a biometric infrastructure, ensure vendor independence, and enable migration to newly emerging technologies, the agencies require the development of a single biometric API. It is hoped that such an API will accomplish the following objectives:

- Provide a comprehensive support for multiple biometric technologies in a common framework (i.e., create a software framework that supports choice of the right biometric for the job, layering of biometrics, and multiple applications sharing a common biometric);

- Provide a robust security architecture for biometrics;
- Provide a standard across multiple platforms and applications; and
- Provide a vendor independent process for development and ownership, supporting the use of interchangeable and interoperable products from multiple vendors.

From the agencies' perspective, the following characteristics shall be required in the envisioned API:

- Multiple levels of interfaces from simple to complex and flexible;
- An extensible framework capable of equitably supporting a comprehensive set of biometrics;
- A common set of cross-biometric terminology;
- A common set of message flows;
- A common set of functions/commands capable of working across biometric technologies;
- An ability to tag biometric objects;
- A platform to support standardization of biometric objects;
- A comprehensive scoring mechanism to support verification and identification;
- Secure transport of biometric data;
- Support for multiple languages (e.g., C, C++, JAVA, etc.); and
- Support for multiple platforms and cross-platform solutions.

Currently there exists a proliferation of generic APIs that have been developed through various strategic alliances and consortia of industry players. These competing APIs have been vying for industry recognition and adoption. However, the Smart Access Common ID Card will adopt a single API. The Biometric API adopted by the Smart Access Common ID Card shall be the BioAPI, developed by the BioAPI Consortium.

2.4.2 Digital Signature/Certificates

In the generation of digital signatures and verification of digital certificates, it is the intent of GSA to assure that sufficiently robust cryptography is provided to agencies requiring this functionality. By adhering to industry supported standards, GSA hopes to allow an agency/application to process certificates from different Certificate Authorities in the same manner, thereby encouraging agencies to competitively procure Certificate Authority services and reducing an agency's dependence on a particular service provider. The technical requirements described below are meant to provide guidelines without restricting the development of emerging technologies in this area.

2.4.2.1 Key Lengths

In general, the agency shall require each public key associated with a certificate to have a minimum of 1024 bits. However, if alternative key lengths are required by individual agencies, then only implementations using alternative key lengths that have been evaluated in accordance with FIPS 140-1 Level 2 may be offered.

2.4.2.2 Algorithms

The standard mandatory algorithm proposed for government use is the RSA digital signature algorithm that adheres to: RSA “PKCS #1: RSA Encryption Standards” Version 1.5, RSADSI, November 1992 signature algorithm. PKCS #1 describes a method for encrypting data using the RSA public-key cryptosystem. Agencies shall use this algorithm in the construction of digital signatures and digital envelopes. For digital signatures, the content to be signed shall first be reduced to a message digest with a message digest algorithm, and then the message digest shall be encrypted with the RSA private key of the signer of the content. The content and the encrypted message digest shall be represented together to yield a digital signature. For digital envelopes, the content to be enveloped shall first be encrypted under a content-encryption key with a content encryption algorithm (such as DES), and then the content-encryption key shall be encrypted with the RSA public key of the recipient(s) of the content. The encrypted content and the encrypted content encryption key shall be represented together to yield a digital envelope.

Alternatively, agencies may choose to adopt other optional algorithms. If the Digital Signature Algorithm is selected, it shall adhere to DSA, FIPS Publication 186-1, Digital Signature Standard (DSS), National Institute of Standards and Technology, (NIST), May 1994.

2.4.2.3 Hashing Algorithms

The recommended mandatory hashing algorithm shall be the Standard Hash Algorithm (SHA) that adheres to FIPS Pub 180-1, Secure Hash Standard (SHS), NIST, April 1995.

Another optional hashing algorithm that may be considered is Message Digest 5 (MD5) that is in conformance with IAW RFC 1321, the MD5 Message-Digest Algorithm, Internet Activities Board, April 1992.

2.4.2.4 Key Generation/Protection

The government recommended mandatory key generation method is for keys used in RSA that shall follow PKCS#1: RSA Encryption Standards, Versions 1.5, November 1992, Section 6, Key Generation.

Alternatively, an agency may adopt the optional DSA and shall conform to IAW FIPS Publication 186-1, Digital Signature Standard (DSS), National Institute of Standards and Technology (NIST), May 1994, Appendix 3, Random Number Generation for DSA.

For alternate algorithms, only government-approved key generation mechanisms shall be used.

The agencies shall adopt Government-approved guidelines for individuals and entity representatives regarding the due diligence and prudence for protection of the private keys. The agency designated Certificate Authority shall protect its private key in accordance with its specified Certificate Policy and Certificate Practice Statement. Keys generated by agency designated Certificate Authorities shall conform to Level 2 Key Management as defined by FIPS PUB 140-1.

2.4.2.5 Certificate Format

According to the *Guidelines for Placing Biometrics in Smart Cards*: "Certificates are portable blocks of data, arranged in a standardized format, which are often used to provide identification. X.509 Version 3 is the ISO (International Organization for Standardization) standard for certificates. X.509 certificates can be separated into two basic categories: public key certificates and attribute certificates. In public key certificates, the primary piece of data being conveyed is a public key. Attribute certificates are much like public key certificates, with the difference being that instead of carrying a public key, the certificate's primary payload is some other form of data (such as a biometric template)".[20] For public key certificates, the agency designated Certificate Authority shall create and maintain certificates that conform to X.509 Version 3 Certificate format as stipulated by the following:

- IETF PKIX Working Group, "Internet X.509 Public Key Infrastructure Certificate and CRL Profile (RFC2459), January, 1999. (this draft standard updates ITUS-T Recommendation X.509, "The Directory Authentications Framework" June 1997).

The recommended certificate format shall include the required fields stipulated in Table C.3.4.2 Required Certificate Fields of the Access Certificates for Electronic Services(ACES) Request For Proposals.[21] The recommended fields for the X.509 Version 3 certificate are delineated in Appendix B of this document. The naming conventions used for X.509 VERSION 3 certificates are included in the chart in Appendix B.

Attribute certificates (e.g. biometric certificates), used to convey a set of attributes along with a public key certificate identifier or subject name, shall conform to the ANSI X9.57 standard.

2.4.2.6 Hardware/Equipment

The hardware tokens and readers used by agencies shall conform to and support the following standards:

- Public Key Cryptography Standard (PKCS) #11: "Cryptographic Token Interface Standard," Version 1 RSADSI, April, 1997; and
- Cryptographic Module Protection – FIPS PUB 140-1 Level 2.

2.5 Card Issuance Equipment

Enrollment workstations (with imaging capability) and related photo, biometric, and signature image capture equipment necessary to perform the required functions in each of the agency designated card issuance locations shall be needed. Additionally, the enrollment workstation

[20] *Guidelines for Placing Biometrics in Smartcards*, Op. Cit., p. 3-4.
[21] U.S. General Services Administration, Federal Telecommunications Service, Office of Information Security, Access Certificates for Electronic Services (ACES) Request For Proposals (RFP) Multiple Award Schedule (MAS)TIBA98003A, January 4, 1999, p. C-19-22.

shall be able to be linked through networking capability to certificate generation workstations maintained by the Certificate Authority and the Attribute Authority.

Workstation application software necessary to support the functions of the Smart Access Common ID Card and its agency designated applications shall be developed and installed. These workstations shall be used initially to capture the digital image of the cardholder’s signature and color photo, certain demographic information, provide local secure and redundant storage of images, and transport the data and images to the central card system. Additionally, the imaging workstation must be able to capture token generated private/public key pairs and biometric templates and transmit this information to Certificate and Attribute Authority systems. Furthermore, should an agency opt to use software generated key pairs, rather than token generated key pairs, an optional key generation system may need to be added to the card issuance equipment configuration.

The enrollment workstations must provide the capability for an authorized user to input client information, capture biometric and photographic images, create biometric templates to be stored on a card, and securely receive and transmit card generated public/private key pairs. Imaging workstations must be capable of processing a complete new client record including data input, formatting, and record transmission in less than 3 minutes on average, and not more than 5 minutes for any client.

At agency option, the workstation configuration must additionally include equipment necessary for over-the-counter card issuance at designated locations. Over-the-counter card issuance would necessarily require card personalization and printing equipment sufficient to meet the requirements of card personalization and issuance processes described in Sections 3.1.2 and 3.1.3.

Depending on the proposed solution, workstations may also require an interface directly with the central card management system, as well as with repositories maintained by the designated Certificate Authority and Attribute Authority. The workstations must confirm receipt of record transmission at the central card management system, as well as at the Certificate Authority, and the Attribute Authority system prior to deleting records from temporary storage in the originating workstation.

The agencies require an approach for configuring the enrollment workstation and components. This approach shall consider appropriate operating procedures and installation considerations (equipment layout, footprint, environmental requirements, etc.). The workstations must be compliant with the Americans with Disabilities Act (ADA).

On average, the workstations must provide 100% functional capability at least 99.5% of the time during agency application office business hours. The number of required enrollment workstations will vary depending on the unique requirements and card issuance strategies of each agency.

2.5.1 Enrollment Workstation

The agencies anticipate that new equipment consistent with modern office environments will be needed. As of the time that this document was released, a minimal workstation configuration shall include:

- Full 32 bit multi-user, multi-tasking, multi-threaded operating system;
- A minimum processor configuration of 300 MHz;
- 64 MB RAM;
- Two (2) hard drives of at least 4GB each to provide for back-up of workstation operating capability and for redundant storage of images. Each drive must have sufficient capacity to archive three weeks activity;
- 256 KB external cache (expandable to 512 KB);
- 3.25" diskette drive;
- 17" SVGA non-interlaced monitor capable of multisync/multiscan resolution of up to at least 1024 X 768, non-interlaced at this resolution and with a dot pitch of .28mm or better;
- Either a network interface card or an internal modem that is capable of supporting a high-speed dial-up communications link with the central card system and Certificate and/or Attribute Authority, if applicable, over commercial telephone lines.

However, it is incumbent upon the vendor to provide technology commensurate with the "state of the art" of the industry at the time the services are procured by the agencies. GSA shall expect that vendors will provide equipment that is consistent with ongoing upgrades in technology.

2.5.2 Video/Digital Camera

A video/digital camera shall be interfaced with each workstation to support the requirements for the capture and storage of a digitized color photograph. The enrollment workstation shall provide the interactive controls and capability for an operator to take and store a color digital photo image of applicants. The operator shall be able to:

- Collect color photograph images via a direct electronic input from an interfaced video/digital camera;
- Control operation of the camera from the workstation;
- Display the photo image on the workstation display monitor in live-digital mode to allow the operator to view and adjust positioning, lighting and focus prior to photo image capture;
- Easily recapture photo images if the operator judges that the captured image is unacceptable;
- Not include a photo image in the identification record and annotate the record to clearly indicate the reason that the data is not included (e.g., religious prohibition).

The camera shall have adjustable height capability and shall allow for the photographing of seated customers with the camera either free standing or positioned on the standard work counter which is between 38 and 43 inches from the floor. The photo installation at any agency application office must include a monochrome background and a standard lighting system to ensure the quality and uniformity of the photo images.

The video/digital cameras shall be able to record the employee's picture in an industry standard bit map file format. The camera shall be capable of capturing high quality colored images and at a minimum shall support the 300 DPI resolution required by the card printers.

2.5.3 Digitized Signature Capture Device

A written signature capture device may be interfaced with each workstation. If included, the imaging workstation shall provide the interactive controls and capability for an operator to take and store a digital image of the applicant's written signature. The signature image shall be captured via direct electronic input from the signature capture device.

2.5.4 Biometric Capture Device

The imaging workstation may have an interfaced biometric scanner. If a biometric scanner is included, the enrollment workstations shall provide the interactive controls and capabilities for an operator to:

- Collect biometric images via a direct scan of biometric features;
- Control operation of the biometric scanner from the workstation;
- Display the biometric image on the workstation display monitor to allow the operator to view biometric positioning and image quality;
- Easily recapture images that were incorrectly positioned, or were rejected by the workstation's automatic image quality analysis; and
- Include biometric image quality information in the biometric image record.

The biometric scanner must be able to support extensive quality assurance capabilities including:

- Ability to perform an automatic assessment of the quality of each biometric image and notify the workstation operator that biometric image data entered are either acceptable or unacceptable for use to perform a match;
- Ability to allow the workstation operator to re-enter images and modify any client record data prior to creating the enrollment template; and
- Ability to flag the image as poor quality and include the best of the three images in the record after three unsuccessful attempts to capture an image that passes the workstation's quality test (no more than 1% of all images may be flagged as having poor quality).

2.5.5 Card Printer

Card printers shall be provided that automatically produce, without operator intervention, high quality, durable cards, as a seamless operation with all chip, magnetic stripe information, graphics, and protective laminate applied. The security of the card shall optionally be protected by holographic images in the laminate (with the substrate visible under normal light) and the laminate shall be fused across the entire (top) face of the card. High quality colored graphic images, at a minimum resolution of 300 dots per inch (DPI), shall be produced by the printers that shall use an approved dye-sublimation process. At a minimum, the printer shall be capable of printing graphics on the entire card, edge to edge, and shall be able to print on both sides of the card. Printing of cards shall be restricted to authorized staff.

2.5.6 Card Reader/Writer

The imaging workstation shall provide an interface with a card access device that allows data to be read from and written to the card. The card acceptance device interfaced with the enrollment workstation shall be in compliance with Section 9 of the *Government Smart Card Technical Interoperability Guidelines*.[22]

2.5.7 Key Generation Workstation

At the agency's option, key pairs may be software generated rather than token generated. If such a solution is required, a secure workstation equipped with a cryptoprocessor shall be available to generate public/private key pairs. A secure means to transmit these key pairs to the imaging workstation for insertion on the card shall be provided.

2.6 Card Acceptance Devices

The agencies require card acceptance devices that are capable of reading each of the technologies included on the card. However, it is not expected that one reader will read all possible technologies that may be on the Smart Access Common ID Card. Integrated circuit chip readers must be able to read and write to the card using either a contact or contactless interface. The card acceptance devices must be in compliance with Section 9 of the *Government Smart Card Interoperability Guidelines.* Card acceptance devices used to read remote coupled contactless cards that conform to ISO 14433 shall be able to read both Type A and Type B formats.

2.7 Physical Access Control Devices

The physical access control system is comprised of the following hardware and software components that are linked through a communications capability:

- Card reader;
- Local access panel/controller;
- Host CPU/File Server
- Client workstations;
- Access control software;
- Access devices including turnstiles, gates, portals, locking devices, and other access control equipment.

The communications capability linking these components shall be compatible with the existing communications infrastructure of the requesting agencies. The network used shall be configured to be fully redundant to ensure continuous 24 hour a day, seven day a week operation and to prevent a communications outage resulting from a single point of failure. Standard communication protocols and equipment shall be used.

[22] *Government Smart Card Technical Interoperability Guidelines,* Op. Cit., p. 61-63.

At agency discretion, a biometric may be used as an access device.

2.7.1 Card Reader

The type of card reader shall be determined by the technology of the physical access control system (e.g., contact or contactless chip, proximity, Wiegand, or magnetic stripe). If a smart card reader is required, it must meet the ISO 7816 – 1/2/3 standards and use T=0 or T=1 protocol for communications.[23] Each reader shall be interfaced to a local access panel/controller and shall be powered directly from the controller. External or local power supplies shall not be required unless the reader electronics is located more than 1000 feet from the controller.

Readers for smart card based physical access control systems either may be programmable or pass through. Pass-through readers are better suited for on-line systems, where the host provides sufficient processing power. Programmable readers are best suited for off-line systems, on-line systems in which the host capabilities are unclear, and for systems that project a need for future flexibility. One of the main benefits of programmable readers is that they perform verification (biometrics or password) at the reader level and thus enhance the privacy and security of the system. A pass-through reader must transmit the PIN, password, or biometrics information across the network to the host computer, whereas the programmable reader can handle the information internally or locally.[24]

Optionally, the card reader shall include a key pad to allow entry of a user PIN. It shall also optionally include a LCD display for displaying special user-configured messages in conjunction with access requests. Depending on the operation of the physical access control system, the reader may also have a reader escort light that provides a go/no go signal for guard gate locations.

If readers are to be used indoors at room temperatures, one built with standard commercial grade electronic components shall be sufficient. However, if readers are to be placed outdoors, in a range of temperatures between –40° Fahrenheit and 125° Fahrenheit, industrial grade components shall be used. Outdoor readers shall be enclosed within a mounting box with a door to protect the reader from exposure to moisture. However, if a contactless chip is used, the mounting box should not require the door to be opened for use.

Readers to be used with a physical access control system shall be placed in conformance with the Americans with Disability Act (ADA).

2.7.2 Local Access Panel/Controller

The Local Access Panel/Controller (LAP/C) is a device that combines intelligent local processing capability with downloaded database processing. Called different names in different products (e.g., remote processing controller, networked intelligent controller, etc.), the LAP/C

[23] 3-G International., *Smart Card Access Control*, p. 26.
[24] Ibid., p. 36.

shall communicate, control, collect, and store data and messages from the existing field devices and send the data to the host. The LAP/C shall have the capability to be connected via a multi-drop communications link directly to the CPU through any of its serial ports or via a TCP/IP network. Alternatively, it may be connected via modem or over dial-up communications to the CPU.

These LAP/C devices shall store cardholder data, remote alarm point information (if an optional alarm system is connected to the system), and transaction records. It may provide local processing based on the full local storage of cardholder records with PIN assignments, access groups, area authorizations, time zones, and activation/deactivation dates. The LAP/C shall be capable of performing its tasks independent of the host processor. Each LAP/C shall monitor and control a cluster of card readers in a multidrop configuration. It shall be able to make access decisions and provide appropriate out point control based on time of day, date, card presentation, keypad presentation, and/or security operator command or door lock override key switch. It shall have sufficient storage capability to maintain records of all transactions.

During a power or communications outage, the LAP/C shall be capable of performing all of the routine security functions of access control, based on parameters established by the system administrator and downloaded from the CPU. It shall be capable of full local storage of event transactions if the controller loses communication with the host/file server computer. The LAP/C maintains a history of all transactions that take place while communications are interrupted. When communications are restored, LAP/C uploads the transaction to the CPU for inclusion in the system history files and archives.

The LAP/C shall be UL listed as conforming to Underwriters Laboratories 294 and 1076 and utilize a UL listed Uninterruptable Power Supply (UPS) that shall be mounted in the LAP/C’s standard enclosure. During a power outage, the LAP/C’s own UPS power supply shall provide power not only for panel operation, but also for the readers, electric strikes, alarm monitor modules (if an optional alarm system is connected to the system), and relay modules which are connected to it. The battery back-up shall provide back-up power for a minimum of four hours. The LAP/C shall also conform to the standards and practices of the National Electrical Code.

Multiple card technologies shall be able to be supported on the same panel. The LAP/C shall be able to support different card formats (e.g., UIC, SEIWG, DOE, and other spec card formats).

2.7.3 Access Control Software

The access control software is the collection of programs that operates the physical access control system components. It shall include, but not be limited to the software required to perform the following functionality:

- Access control;
- Database management; and
- System configuration.

The access control software shall be a menu-driven, open architecture design that shall support the following features:

- Capability to synchronize databases between the host database and the LAP/C user access database;
- Use of a full 32 bit multi-user, multi-tasking, multi-threaded operating system that allows the system to control and monitor card readers, and support multiple concurrent tasks without degradation in the overall system performance;
- Capability to run under multiple operating systems (e.g., Windows NT, IBM OS/2, etc.);
- On-line user and operator manual, with complete context sensitive help facility;
- Central or distributed transaction processing for the complete database;
- Ability to implement anti-passback/anti-tailgate capability;
- Configurable, automatic time zone controlled commands;
- Configurable, automatic time controlled report generation and/or disk back-up commands;
- History/audit trail of all transactions;
- Encrypted, secure transactions between the host and the LAP/C;
- Partitioned database that allows the system administrator to restrict access to menus and records for designated operator groups;
- Monitored and displayed system activity to allow the system administrator to diagnose poorly running systems and dynamically tune system operations;
- Generation of LCD displays at individual card readers based on specific cards or keypad input;
- Concurrent running of other programs while operating access control software;
- Comprehensive report generator for retrieving and reporting on system history and database transactions;
- ODBC compatibility to allow physical access control system to be integrated with commercially available database management packages;
- Upload/download capability to import data from external computer systems;
- Scalability to easily increase the number of cardholders, card readers, and workstations;
- Graphical User Interface;
- Simultaneous usage of administration, event monitoring, and status windows;
- Separate visitor database and visitor control functionality;
- Automatic card activation and deactivation based on time/date and usage;
- Access activity analysis by card reader or security area;
- Variable card formats;
- User defined remote control functions;
- Multiple site and facility codes; and
- Remote diagnostics capability (including the capability to protect the remote diagnostic port on the server containing the access control software).

2.7.4 Host/File Server

The host or file server is composed of the computer CPU, keyboard, color monitor, and required software. The host shall support remote workstation access via communication connections, and provide dial-in capabilities to perform all system administration functions.

The agency will specify their host or file server configuration requirements. However, at the time that this document is released, it is anticipated that these will include, at a minimum:

- A minimum processor configuration of 300 MHz supporting true multi-user, multi-tasking and multi-threaded capabilities;
- 64 MB of RAM, expandable to 128 MB of RAM;
- Five serial I/O ports (expandable up to 127);
- Two parallel ports;
- Capable of supporting two printers;
- 15” Color monitor;
- Standard 101-key keyboard;
- Two button Mouse;
- Full 32 bit multi-user, multi-tasking, multi-threaded operating system;
- Network Interface Card capable of supporting multiple network protocols such as TCP/IP, IPX/SPX, and NetBeui concurrently;
- Three GB fixed hard drive; and
- Floppy disk, tape drive, or removable zip drive for archiving; and
- Support up to 32 fully functional workstations.

It is incumbent upon the vendor to provide technology commensurate with the “state of the art” of the industry at the time the services are procured by the agencies. GSA shall expect that vendors will provide equipment that is consistent with ongoing upgrades in technology.

The host shall provide redundant processing to assure 100% availability. There shall be available a primary host and a secondary (hot standby) which shall be located in a remote location or separate building. Both hosts shall be connected to local area communications facilities. The primary and secondary host shall each maintain identical mirrored images of the database that will be updated at both host locations in real-time. In the event of a failure of the primary host, the secondary host shall immediately take over the operation with no human intervention.

2.7.5 Client Workstation

There shall be one or more client workstations to provide database entry, operator requested reports, and, if included in the physical access control functionality, alarm/event reporting. The operator interface shall be menu driven through easy to understand menus, text, and prompts. The client workstations shall communicate with the host (file server) over an industry standard LAN.

The client workstation shall be configured, at a minimum, to include:

- A minimum processor configuration of 300 MHz supporting true multi-user, multi-tasking and multi-threaded capabilities;
- 64 MB of RAM, expandable to 128 MB of RAM;
- Two serial I/O ports (expandable to four or more);
- Two parallel ports;
- Capable of supporting two printers;
- 15” Color monitor;
- Standard 101-key keyboard;
- Two button Mouse;
- Full 32 bit multi-user, multi-tasking, multi-threaded operating system (e.g., Windows NT or IBM OS/2);
- Network Interface Card capable of supporting multiple network protocols such as TCP/IP, IPX/SPX, and NetBeui concurrently; and
- Capable of running operator software package.

2.7.6 Locking Devices

Electric locking devices shall be provided to lock and unlock each card reader controller door and auxiliary door. These locking devices shall be able to be controlled through local access panels/controllers that route access approval transactions to activate the locking devices.

2.7.7 Turnstiles/Gates

Turnstiles or gates may be optionally used to provide or deny access at a main entry. These turnstiles or gates shall provide mechanical barrier control. The turnstiles or gates shall be able to be controlled through local access panels/controllers that route access approval transactions to activate these physical devices.

2.7.8 Optical Turnstiles

Optical turnstiles may be optionally used to provide or deny access at a main entry access point. These turnstiles provide barrier control based on optical (e.g., infrared) signals. These turnstiles shall be able to be controlled through local access panels/controllers that route access approval transactions that generate optical signals.

2.7.9 Revolving Security Doors/”Mantraps”

The revolving security doors or “mantraps” provide the capability to ‘capture’ an individual within the doorway until the individual’s identity is authenticated and access status is verified. This process is highly effective in preventing “tailgating” and is generally used by agencies requiring high levels of security. The mantrap control software shall incorporate the use of a weight comparison with user definable weight thresholds, measured by a weight scale internally in the mantrap, and a biometric device internal or external to the mantrap.

2.7.10 Portals

Portals provide the ability to simultaneously perform both physical access control and asset protection. As the user walks through a portal, the electronic interface in the portal shall read the proximity or contactless chip card. At the same time, the portal shall be able to detect the presence of radio frequency tags inserted in assets in the possession of the cardholder. The portal shall read the card as well as the RF tag, create a transaction to query the local controller or host to verify the access and asset assignment designation, and sound an alarm if the asset is not linked to the respective cardholder.

2.7.11 Additional Physical Access Control System Technical Requirements

In the event of a power failure or high/low temperature condition, the physical access control system shall shut down in an orderly fashion to prepare for an automatic restart, and shall execute an auto-restart after the power or temperature condition is corrected.

Back-up power shall be provided for uninterrupted operation of system computer and communications equipment and printers. This back-up power shall be provided by computer grade, on-line Uninterruptable Power Supply units (UPS), which shall supply continuous no-break power. Each UPS shall consist of, but not be limited to, a rectifier, batteries, support racks, or enclosures, static inverter, static transfer switch, manual bypass switch, and suitable overcurrent protection devices, in accordance with applicable electrical codes. Each UPS shall have a continuous output to supply the maximum load requirements of the support equipment. Battery capacity shall be sized to sustain the supported equipment at full load for four (4) hours. Each UPS shall include the following features:

- Pure sine-wave regulated output, less than 5% total harmonic distortion. The output voltage shall be regulated to 3% meeting standards set by ANSI c84.1;
- Brown out protection;
- Lighting and surge protection meeting ANSI/IEEE C62.41 Categories A and B;
- Temperature-compensated charger;
- Automatic battery replace warning, inverter check, runtime monitoring, and shutdown;
- Isolation of output neutral, meeting requirements of true, separately derived power source as defined by the National Electric Code Article 250-5d;
- Sealed, VRLA or Nickel Cadmium no maintenance batteries, with a rated life expectancy of 10 years, to provide 4 hour running time for the maximum loads anticipated at the UPS;
- Rated for switch-mode power supplies; and
- For connection to circuits backed by emergency generators, UPS shall be suitable for use with emergency generator circuits, with appropriate filtering circuits to prevent UPS drop-out as the generator comes up to speed.

All of the junction boxes, terminal cabinets, and equipment enclosures shall be NEMA 4X stainless steel. The junction boxes shall be sized per the National Electrical Code. All junction boxes, terminal cabinets, and equipment enclosures shall be equipped with stainless steel tamper-proof closure screws and hardware, and with continuous hinge covers. Interior and exterior equipment enclosures shall be equipped with heavy duty, stainless steel pad locking hardware. All equipment enclosures and terminal cabinets shall be equipped with individually circuited tamper switches. All equipment enclosures shall be equipped with three point latching hardware and keyed locking hardware keyed to match standard facility lock systems.

2.8 Logical Access Control Devices

In addition to the Smart Access Common ID Card (refer to section 2.2), additional hardware devices required to support logical access control will include a card read/write device and may also include a PIN pad and a biometric verification device.

2.8.1 Card Reader

The logical access control card reader is the interface between the Smart Access Common ID Card and the workstation or computer device in use by the cardholder. The logical access control card reader shall be capable of reading smart cards that conform to the specified ISO standards specified in this document. For purposes of logical access control, the card reader shall communicate with the Smart Access Common ID Card through the card's contact interface. The card reader may be built directly into the workstation or may be connected via a communications port or other special purpose interface. If the card reader is not built directly into the workstation, any communications between the Smart Access Common ID Card and the workstation shall be encrypted. Depending on the cardholder's access privileges, the card and reader may be used to control the user's access to the sign-on workstation, other workstations, specific databases and/or the enterprise host systems. Access may occur through Intranets, extranets, dial-up modems, or virtual private networks (VPNs) such as the Internet.

Card reader specifications shall be determined by the agency and the specifications shall vary depending on the physical operating environment, the level of required security, the capabilities of the workstation, and whether access request originates from a local or a remote user location. In order to support encryption, biometric verification, and PIN verification, the card reader shall be programmable. Depending on the agency's specific requirements, the reader shall also optionally include a LCD display, a light, or emit audible sounds to allow for instruction or feedback to the user.

2.8.2 PIN Verification Device

If logical access control functionality includes the use of PIN or Password to authenticate the individual cardholder, a PIN or Password verification terminal with encryption capability shall be required. Under no circumstances may a PIN or Password be transmitted between the card and the verification terminal in the clear. Password usage must be in compliance with FIPS PUB 112, *Password Usage*.[25]

[25] FPIS Publication 112, *Password Usage,* May 30, 1995.

2.8.3 Biometric Verification Device

If logical access control functionality includes the use of biometric verification to authenticate the individual, a biometric verification terminal shall be provided. The biometric verification device may be built into the workstation or reader or may be connected through a communications port. The biometric verification device shall scan the physical feature presented and convert the scanned image to a digital template which shall be compared to the digital biometric template stored on the Smart Access Common ID Card. Biometric verification must meet the operating requirements and performance standards specified in this document. Use of biometrics for logical access control must be in compliance with FIPS PUB 190, *Guidelines for use of Advance Authentication Technology Alternatives.*

2.9 Maintenance

The agencies require that maintenance be available on all workstations, peripherals and card interface devices that are deployed to support the Smart Access Common ID Card. An inventory of workstations and peripherals shall be maintained to swap out malfunctioning equipment. The terms and hours of maintenance services shall be determined by each contracting agency.

2.10 Interface Requirements

Interfaces with legacy systems shall be required to retrieve information needed to support Smart Access Common ID Card issuance and to provide notification of card replacement or status activity. Additional interfaces may be required between the central card system and/or enrollment workstation and the Certificate Authority systems. Further interfaces with agency legacy systems may be required for identity proofing. Interfaces may also be required between the central card system and/or enrollment workstation and the Attribute Authority systems to provide biometric enrollment and verification.

In support of the agency designated optional applications on the card, an individual agency may need to implement interfaces between its central card system and/or enrollment workstation and the existing agency application systems. The requirements for systems integration will be dependent upon the options exercised by and specific requirements of individual agencies.

2.11 Year 2000 Compliance

The agencies require that the respective vendor team(s) represent and warrant that all hardware and software products which are supplied to them by the vendor team(s) are designed and intended to be used prior to, during, and after the calendar year 2000 A.D. The agencies require that the products have been designed to ensure year 2000 compatibility, including, but not limited to, date data century recognition, calculations which accommodate same century and multi-century formulas and date values, date data century display formats and date data interface values that reflect the century. Additionally, all hardware and software products supplied to the agency shall be in compliance with the specifications in Section 6.9 of the *Government Smart Card Technical Interoperability Guidelines*.[26]

[26] *Government Smart Card Technical Interoperability Guidelines*, Op. Cit., p. 30-31.

2.12 Compliance with Regulations/Legislation

The agencies shall comply with agency regulations or Federal Legislation (e.g., Federal Privacy Act, Government Paperwork Elimination Act, etc.) and any other legislation or regulatory requirements that impact the procurement and implementation of the Smart Access Common ID Card.

3 MANDATORY FUNCTIONAL REQUIREMENTS

3.1 Card Management System

The agency must ensure that responsibility is assumed for all facets of card management including card procurement, inventory control, personalization, issuing, and card replacement. The agencies require procurement and issuance strategies to ensure that the Smart Access Common ID Card is produced and issued in a cost-effective and secure manner.

The agency shall either assume responsibility for, or shall designate an entity to implement a card management system to manage and track the functions required under card management.

3.1.1 Card Procurement

The agency or its designated card issuer shall procure cards from one or more specified card manufacturers. The cards shall have all the capabilities specified in this *Preliminary Requirements Document* and shall be produced according to the designs developed under the auspices of the individual agency and the agency's designated entity. Smart cards procured by different agencies shall comply with not only this requirements document, but also with the *Technical Interoperability Guidelines* document, which should ensure some level of technical interoperability. This document does not intend to cover visual card design/artwork, which may vary to distinguish cards by some discriminating factor, such as: agency, intended use, authorization level, or other factors.

The manufacturer must encode the chip with a unique serial number. Each serial number shall be associated with a single cardholder. The agency shall ensure that card management includes an approach for adequately sizing the chip. This approach may include a plan to either procure cards with a standard size (memory capacity) chip or to migrate to chips with greater capacity as the need arises.

The card manufacturer shall replace defective cards at no cost to the agency.

3.1.2 Card Initialization

The agencies shall opt either to issue Smart Access Common ID Cards or to designate a card issuer to issue the cards on their behalf. The agency or its designated entity shall arrange for initialization of cards. For the card initialization process, the card vendor shall perform such functions as:

- Loading the operating system into ROM;
- Allocating memory zones on the chip (e.g. for photo, for digital signature);
- Loading the unique card serial number into ROM;
- Generating security keys; and
- Other card initiation tasks as requested by the agency, or its delegate.

3.1.3 Card Personalization

Prior to issuance, the agency or its designated card issuer shall be responsible for ensuring that cards are initialized and personalized. For the Smart Access Common ID Card, the personalization processes may include some combination of the following depending on which applications are being loaded on the card:

- Encoding the magnetic stripe;
- Encoding the bar code;
- Loading application software, basic demographic information and/or keys to the chip;
- Printing card graphics;
- Printing photo and signature image on the card;
- Printing demographic data on the card; and
- Printing other agency specific information on the card.

Agencies may employ various approaches for obtaining data for the card personalization process. Downloads from existing legacy systems, Web-based applications to collect data, or employee interviews are examples of techniques that may be used to obtain necessary card personalization data. Once these data are collected, interfaces may be built in order to efficiently enter the data into a master or legacy database.

In addition, if an agency opts to add other applications to a card already in circulation, the agency or its designated card issuer shall develop methods for loading new applications to the card. The agency or its designated card issuer shall use a standard methodology for adding additional applications to the card, as well as a specified process for registering application identifiers.

As part of the enrollment and card personalization process, the agency or its designated card issuer shall perform some combination of the following functions:

- Capture the digital photograph of the employee using the photo imaging system;
- Capture the digitized signature of the employee using a signature capture device;
- Capture the biometric of the employee using a biometric capture device;
- Capture demographic data to be maintained in the cardholder database and write this demographic data to the chip; and
- Populate the card with digital and attribute (i.e., biometric) certificates.

The requirements for these functions are further described in the subsections below.

3.1.3.1 Photo Image Capture

The agency or its designated entity shall capture the cardholders digital image through its imaging workstation and video/digital camera. At the discretion of the agency, the digitized image may be stored in the central card system.

3.1.3.2 Digitized Signature Capture

At agency discretion, an image of the cardholder's written signature may appear on the face of the Smart Access Common ID Card. This image may be captured from a direct capture electronic device. The image of the written signature may be stored on the Central Card System and may also be stored on the chip on the cardholder's Smart Access Common ID Card.

3.1.3.3 Demographic Data Population

The demographic information shall be obtained from the applicant and encoded on the integrated circuit chip as part of the card personalization process. This information shall reside in a common area and shall be accessible by all applications. At agency discretion, this demographic data may be obtained by downloads from existing databases, through an enrollment interview with the applicant, or through other means acceptable to the agency.

3.1.3.4 Digital Certificate Population/Key Pair Generation

Agencies may choose various options for generating and populating the card with the digital certificate as part of the card personalization process. If the agency chooses to function as its own Registration Authority (see Glossary in Appendix A) but contract with a Certificate Authority (see Glossary in Appendix A) to sign certificates, the agency will generate or obtain public/private key pairs for each smart card to be registered. The agency would then submit a secure request to the CA for a formatted and signed digital certificate for each of the public keys that it needs certified. The CA, in turn, shall return a formatted and signed X.509 certificate to be placed on the card during the card personalization process. The certificate shall be placed on the card either through a bulk card personalization process or an over-the-counter enrollment station.

If the agency chooses to function as its own Registration Authority and Certificate Authority, the processes of performing identity proofing, generating key pairs, generating digital certificates for public keys, and placing digital certificates on the card shall be performed in-house as part of the card personalization process. In this scenario, the agency shall provide a secure system to issue and manage digital certificates, as well as to populate the card during the personalization process.

3.1.3.5 Attribute Certificate Population

Agencies may choose various options for generating and populating the card with the attribute certificate as part of the card personalization process. Many agencies are likely to use the same entity to function as both a Certificate Authority and an Attribute Authority. If the agency chooses to function as its own Registration Authority but contract with a Attribute Authority (AA) to sign certificates, it shall capture biometric scan information, generate a biometric template, and generate a secure request for a formatted and signed attribute certificate that is sent to the AA. The AA, in turn, shall return a formatted and signed attribute certificate to be placed on the card during the card personalization process. The certificate shall be placed on the card either through a bulk card personalization process or an over-the-counter enrollment station.

If the agency chooses to function as its own Registration Authority and Attribute Authority, the processes of performing identity proofing, generating biometric templates, generating and signing attribute certificates, and placing attribute certificates on the card shall be performed in-house as part of the card personalization process. In this scenario, the agency shall provide a secure system to issue and manage attribute certificates, as well as to populate the card during the personalization process.

3.1.4 Card Issuance

The agencies may choose various options for card personalization. Although cards are expected to be issued to employees in person on-site at agency locations, an agency may opt to have a vendor personalize and print cards from a central location. The option to have the vendor personalize cards from a central location may be used to support mass card distribution. Security tradeoffs should be considered when deciding whether to implement a central issuance, a local issuance or a hybrid issuance scheme. Prior to authorizing a card issuance transaction, the employee will be required to present documentation to verify their identity and employment status. Acceptable forms of identification shall be at the agency's discretion and shall be based upon the rules agreed upon with the agency's designated digital signature and attribute certificate agent. It is important to note that while agency discretion will determine acceptable identity proofing requirements for certificate issuance, it is the receiving agency that will determine the value of the certificate for access privileges away from the home agency. The system is only as strong as its weakest link. If the receiving agency requires rigorous identity proofing for certificate issuance in their system for controlling privileges within their agency, receiving a certificate from an agency who more flippantly issues certificates will probably mean that access privileges will be denied to the token presenter. Reconciliation of the level of trust in various certificate issuance schemes has been addressed by the industry (e.g., CertCo). The vendor must also provide a solution for loading of digital and attribute certificates to the cards that will carry these privileges.

The applications that will be loaded on to the employee's Smart Access Common ID Card shall vary depending on the employee's job description and duties. While all employees will require a card for visual identification and physical access to their duty station, not all employees will require a digital signature or attribute certificate. The card personalization, card issuance, and card management solutions will provide the capability to capture and maintain records on the privileges associated with each employee's card.

Whether the agency chooses central or on-site card personalization, or a combination of both, the vendor shall be required to supply the agency with the appropriate equipment to produce cards that meet the security and functional requirements specified. Cards personalized and printed on-site at an agency location shall meet the same physical card standards, card security, and quality standards as cards personalized and printed at a vendor's central location.

3.1.5 Card Replacement

The Card Management function must include the capability to provide replacements to individuals reporting a lost, stolen or malfunctioning card. When a replacement card is issued, it must carry all the privileges and keys that resided on the original card that is being replaced. The vendor shall develop a solution for providing card replacement functionality that considers the agency's choice for on-site or centralized card personalization and printing. At agency discretion either the agency or its designated card issuer shall have responsibility for the replacement process. The card replacement process shall specify:

- Procedures for re-issuance;
- Procedures for checking hot listed cards;
- Time frame for hot listed cards being activated in the card database;
- Personnel responsible for locking/unlocking cards;
- Procedures for removing hot listed cards from the list;
- Time frame for re-issuance/re-activation of cards; and
- Procedures for restoring value if the card has an electronic purse.

The agency or its designated card issuer shall have the capability to maintain a history of all cards issued to an individual and shall report card replacements to each program agency for which a privilege resides on the card. When accepting a card replacement request over the phone, the agency or its designated entity shall have the capability to use voice passwords to authenticate the caller.

3.1.6 Card Block

The agency or its designated card issuer shall have an approach for invalidating (deactivating) a Smart Access Common ID Card when that card is reported lost or stolen. This approach shall include specification of how the hot card list is to be handled. The agency or its designated card issuer shall have the capability to hot list any card that has been reported lost, stolen or malfunctioning. In addition, the agency or its designated card issuer shall have the means to report hot listed cards to departments having an application resident on the card. The hot list shall be communicated to any other agency that would grant access privileges to cardholders on the hot list. The hot list shall be updated at a frequency acceptable to the agency. The hot list shall use an agency designated card identifier (e.g., Primary Account Number, Social Security Number, card serial number, etc.) to map "hot listed" cards to specific cardholders.

3.1.7 Cardholder Database Management

The vendor solution must provide the capability for the maintenance of a record of all cards issued. This record must link the card serial number to the cardholder, the cardholder's photographic and signature images, digital and attribute certificates, and pertinent information for all applications carried on the card such that a replacement card containing all authorized privileges, data, and keys can be produced for cardholders that report lost, stolen, or malfunctioning cards. It is expected that additional applications will be added to the Smart Access Common ID Card platform over time. The agency will require a strategy for storage, retrieval, retention, integrity, and management of information necessary for the issuance, status, replacement, and audit of Smart Access Common ID Cards. The solution will require the capture and linking of data from a number of sources and must allow for back-up of stored information and means of recovery. The cardholder database shall be ODBC compliant.

3.1.8 Card Inventory Control

The agency requires that systems and procedures be developed to ensure that Smart Access Common ID Card stock is maintained in a secure environment. The agency or its designated card issuer shall record the serial numbers of cards received in inventory. Cards shall be stored in a secure location with access limited to authorized individuals. Card security must be maintained through the card initialization and personalization processes. The vendor shall be responsible for all Smart Access Common ID Cards until they are delivered to the custody of the agency at designated over-the-counter card issuance locations. The agency or its designated card issuer shall be responsible for the following:

- Recording of serial numbers received into inventory and issued from inventory;
- Monitoring inventory levels and requesting additional card stock from the card manufacturer;
- Processing returned or damaged cards for inventory log update and chip failure testing; and
- Maintaining a distributor card database that details the number of cards issued per month, annually by agency, collection status of card failures and chip failures.

To support card issuance at various agency locations, the vendor shall log the serial numbers of all cards sent to agency locations and shall develop and implement a method to track and monitor inventory depletion rates at these locations.

3.1.9 Cardholder Services

The agency or its designated card issuer must perform or acquire customer service related to the Smart Access Common ID Card. A toll free number shall be provided for cardholder telephone inquiries. To serve cardholders the agency or the designated card issuer shall have the capability to provide an Automated Response Unit (ARU), in addition to customer service representatives.

The ARU shall respond initially to all incoming calls. The ARU shall prompt the caller to indicate whether he/she is using a touch-tone telephone. If there is no response, the call shall be automatically transferred to the Customer Service Center.

In addition to the ARU, the agency or the designated card issuer requires a staffed Customer Service Center unit that shall provide personalized responses to caller questions. All calls shall be referred to the Customer Service Center by the ARU, either as an automatic system transfer or upon the caller's selection of "Customer Service Representative" (CSR) from the ARU menu options.

Anticipated client customer services via either the ARU or a CSR include but are not limited to:

- Report a Lost/Stolen Card (Callers selecting "Report a Lost/Stolen Card" from the ARU menu will be transferred immediately to a CSR.);
- Report a malfunctioning card;
- Report unauthorized card use or other breech of security;

- Report an update in demographic data (name change, change of address, etc.);
- Information support for Smart Access Common ID Card applications and services; and
- Card Replacements (Callers selecting "Card Replacement" will be transferred to a CSR for information on card replacement procedures.)

Telephone-based customer service (ARU and customer service representatives) shall be available 24 hours a day, 7 days per week. Performance standards regarding number of rings prior to answer and average time on hold shall be consistent with financial industry standards for customer services. The agency will be able to obtain ARU and Customer Service Center activity data.

The agency may wish to have an internal process to enable the cardholder to report lost, stolen, or malfunctioning cards. At agency discretion, the agency may wish to have all the functionality of the card issuer.

Additionally, the agency designated card issuer shall require Cardholder Training Materials, including descriptions of, at a minimum:

- Basic card usage;
- Card applications;
- Card security and key protection procedures; and
- Privacy safeguards.

3.2 Basic Identification Requirements

In addition to card management, the following are mandatory functions for the Smart Access Common ID Card:

- Basic identity verification;
- Physical access control;
- Logical access control;
- PKI service provision; and
- Biometric-based identity verification.

3.2.1 Identity Verification Functionality

The verification of an employee should be achieved through one of two means, the first being a system of visual verification. The agency shall be able to verify an individual’s physical identity through the use of the card. The printed photo shall act as a mechanism for this verification, which can be performed by a guard or other personnel at a point of physical entry to a building or other facility. The second form of verification can be completed through an automated function. The use of software application and the insertion of the employee’s card into a card reader would accomplish the automated verification process.

3.2.2 Visual Identity Verification Data Elements

Individual agencies may select the data to be printed on the face of the card. While the following subset of data elements typically will be printed on the face of the card, agencies may choose additional elements or opt not to include all of the following:

- Agency name;
- Agency logo;
- Name (first name, middle initial, last name);
- SEIWG identification;
- Date of issuance;
- Date of expiration; and
- Digitized photo.

Since basic demographic information will be required for all applications that reside on an individual’s Smart Access Common ID Card, this data shall be carried on a common area of the chip that can be accessed by all applications.

3.3 Physical Access Control Requirements

The agencies vary substantially in their current physical access control environments and capabilities. Some agencies have made substantial investments in physical access control systems, while others have no automated system in place. Many agencies have an automated physical access control system in their Headquarters Building, but a different system or no system at all in their regional offices. Agencies often have numerous small offices dispersed around the country in GSA leased buildings or private facilities such as shopping centers. The employees in these small leased offices and shared tenancy buildings often use whatever physical access control system is put in place by the building landlord. There is a major issue with interoperability across this vast array of physical access control systems. For those agencies with significant investment in legacy physical access control systems, backward compatibility shall be a requirement to ease the transition to smart card technology and support the migration to evolving standards in the physical access control arena.

Most agencies have a decentralized badge issuance function, with the Headquarters Building in the Washington Metropolitan area taking responsibility for the local employees only and the regional offices performing badge issuance for all the personnel in their respective regions. While a few departments have a centralized badge issuance function (and decision-making authority) for the entire department, most departments allow their sub-units (i.e., the bureaus or operatives) full autonomy in the physical access control/badge issuance arena. Individual bureaus have the responsibility and the decision-making authority for the badge issuance needs of these smaller units. This decentralization of the badge issuance function makes the achievement of standardization and interoperability across agencies challenging, both technically and politically.

While a few agencies (such as Department of Energy) have worked extensively to standardize the departmental badge and badge issuance procedures, most agencies have a significant problem with interoperability of badges even within their own departmental units. The Department of Energy has created a badge issuance standard and is currently striving to achieve interoperability across the divergent physical access control systems in their own facilities.[27] Similarly, the defense and intelligence communities are working on standard specifications and have an on-line system in place that allows some degree of interoperability across the intelligence and defense agencies.[28]

Although it would be impossible to mandate full interoperability and standardization in such an environment, the Smart Access ID Card program shall, at a minimum, require that integrated circuit chip card standards at the physical card level be observed so as to achieve interoperability at the physical card level. Thus, at this lower physical level, data carried on a chip card from one agency could be read by integrated circuit chip readers at another agency. Interoperability at the higher application level, across multiple physical access control system technologies, however, is outside the scope of this effort.

The following sections detail the functionality that a card-based physical access control system must provide.

3.3.1 Physical Access Control Functionality

Although the technical implementation may vary, the functional capabilities of the physical access control system shall be standard across systems. This basic functionality includes:

- Enroll employee;
- Assign access privileges;
- Conduct access control transaction;
- Authorize access;
- Update privileges
- Track/audit accesses;
- Generate access reports;
- Manage card hot list;
- Maintain access database; and
- Manage visitor control.

The sections below detail the requirements for each of these functions. In some instances, if the physical and logical access control databases are integrated, there may be some overlap in the functionality performed by these two applications.

[27] This effort has culminated in the publication of the following badging standard: Office of Safeguards and Security, "DOE Badge Program, Volumes I, II & III," November 18, 1998.

[28] This effort is being spearheaded by the Facilities Protection Committee, sponsored by the Security Policy Board, and includes a number of intelligence and defense organizations, as well as some civilian agencies.

3.3.1.1 Enroll Employee

The employee must be entered into the physical access control system database so that the physical access control application on the Smart Access Common ID Card can be activated. In the past, when badges and physical access control cards were separate, the cardholder might have gone to two separate offices, one to obtain the badge and potentially a second office to receive the access device card, populate the access control system database, and activate the access device token. In some agencies, the badge and the access control card have been integrated so that only one visit to a badge issuance and/or security office is required. In this scenario, the employee's demographic data is collected either through completion of a paper form and manual entry into the physical access control system or through a download from the personnel/security system. Once the basic data has been collected, the employee is issued a badge, which is activated in the physical access control system database.

Within the Smart Access Common ID Card program, different agencies could adopt various card issuance strategies. If a centralized card issuer with whom the agency has a contract issues the card, the badge issuance or security office (or some other agency designated organization) may still function as the local liaison with the contractor card issuer. In this case, the employee shall come to an office that functions as a local point of data collection.

This local office may obtain a digital photograph, digitized signature, biometric capture, and any additional data not already downloaded from the legacy personnel and/or security database. This information shall be uploaded to a bulk card personalization center, where the card shall be produced and populated with key pairs, digital certificates, and attribute certificates. The cards could be mailed directly to the cardholder from this bulk personalization center. Alternatively, the completed cards could be returned to the local office that shall function as the point of local card distribution. In this scenario, the physical access control data could be sent to the physical access control system database as part of the card personalization process or the cardholder, once the card was in-hand, could be directed to the security office to activate the physical access control application.

Alternatively, the entire card issuance process could take place at the local office. In this scenario, the data would be collected, the keys generated locally, the certificates (both digital and attribute) could be sent from the Certificate/Attribute Authorities and loaded onto the card at the local distribution office. Potentially, the physical access system database could also be loaded from this location. Regardless of the sequence of steps or the specific office designated as responsible, the basic functionality shall be to populate the physical access control database with the required employee information and activate the card to grant access to physical facilities.

3.3.1.2 Assign Access Privileges

The system shall provide a capability to assign appropriate access privileges for individual employees or groups of employees. To maintain access privileges, the system shall provide a capability to initially enter and update access privileges in the system's central database. The system shall support assignment of different access privileges that allow restriction of access by:

- Control point;
- Area;
- Tenant;
- Access group;
- Time of the day;
- Day of the week; and
- Any combination of the foregoing.

3.3.1.3 Conduct Access Control Transaction

The physical access control system shall have the capability to read the employee’s card and retrieve an access control card serial number from the card. The card shall be read using whatever technology is supported by the system in question (e.g., contact/contactless chip, proximity, Wiegand, RFID, or magnetic stripe). The reader shall have the capability to format an access request transaction. If a PIN is required for entry, the local card reader device shall be able to prompt for PIN entry, accept the entered PIN, and add the PIN number to the access request transaction prior to sending the access transaction to the local access panel/controller. If a biometric is used, the biometric shall be read and verified against the biometric template on the card prior to the transmission of the access request transaction.

Initially, the access transaction shall be routed to the appropriate local access panel/controller. The card number shall be used to look up the employee in the local access panel/controller database to determine that employee’s access privileges. If the card number is found, the Hot List shall be checked to ensure that the card is not lost or stolen. If the card is valid, not listed on the Hot List, and the access privileges are appropriate for the access request, an access approval transaction shall be generated and routed to the appropriate local access device (e.g., turnstile, gate, locking device, etc). When the local access panel/controller grants access to a valid cardholder, the information shall be transmitted to the host. If a cardholder requesting access is not in accordance with the local access panel/controller database or the cardholder has an invalid status, the local access panel/controller shall query the host to verify the cardholder’s status before denying access. If it is found that a new record exists on the host that allows access, that record shall be added to the local access panel/controller database automatically and access shall be granted.

If access is not granted because the card number is not in the database, the access request is not within the parameters of the cardholder’s access privileges, or the card is located on the Hot List, the system shall generate an access denial transaction. This access denial transaction shall be transmitted to the local access control device.

3.3.1.4 Authorize Access

Once the cardholder has been validated at the local access panel/controller or at the host, an access approval transaction shall be generated. The appropriate local access control device shall receive the transaction. This device may be a door locking mechanism, a turnstile, a gate, a portal or a “mantrap”. The approved access transaction shall trigger an electronic signal to the device that takes appropriate action such as unlocking the door, providing a "go" light signal, or releasing the gate/turnstile/mantrap.

If an access denial transaction is received at the local access control device, the device shall either lock the door or gate/turnstile/mantrap or provide a "no go" light signal. The access device shall provide the capability to display an error message to the cardholder. Under appropriate circumstances, the system shall allow an authorized user to override the system access control mechanism to allow access when the access transaction is not approved.

3.3.1.5 Update Privileges

The physical access control system shall have the capability to update employee access privileges. The system administrator shall have the capability to access an "assign access privileges" screen to manually adjust access privileges. Additionally, if access privileges need to be adjusted for a group of employees, the system shall be able to accept downloaded files of mass access privilege changes.

3.3.1.6 Track/Audit Accesses

The physical access control system shall create audit records for all system activities that are sufficient to enable reconstruction of each event in a transaction, which are protected from alteration or unauthorized access. The system shall be able to display and print activity reports on demand based on the data compiled in the audit records.

These transactions from field devices and terminal inputs shall be maintained at the host database for a period of twelve months (or an alternative period prescribed by the individual agency). After that period, the transactions shall be archived to off-line storage devices. This transaction history shall provide the basis for activity analysis reports and ad hoc inquiries needed to support audit procedures.

3.3.1.7 Generate Access Reports

The physical access control software shall be able to provide a set of standard reports for supporting the facility and management staff during routine and emergency situations. These shall include, at a minimum, system operation reports such as: alarm (if this optional feature is part of the system), incident reports, communications availability and response times, system utilization, trouble reports, event logs, etc. The system shall also provide a report generation facility to allow staff to produce ad hoc reports and inquiries. The system administrator shall have the ability to add any ad hoc report to the Standard Reports GUI interface.

The user shall have the option of displaying the report on the screen, and downloading the file to selected printers. The reports shall be able to track the following including, but not limited to:

- **Machine Availability** - showing the total number of access devices and equipment in service and out of service and the percentage of total equipment in service;
- **Transaction Summary –** showing the total number of access transactions by transaction type;

- **Transaction Detail –** showing a list of all transactions by category; and
- **Employee Activities –** showing all employee interactions with the access control system.

The system shall provide the ability to read and generate reports from previously created archived data at user request.

3.3.1.8 Manage Card Hot List

The employee shall report any card that is lost, stolen, or malfunctioning to the agency designated Customer Service representative. The Customer Service function shall prepare a hot list file of any cards that have been reported lost, stolen or malfunctioning. The agency or its designated card issuer shall coordinate with the physical access control application owner to ensure that the Hot List database is routinely downloaded to the physical access control system host and local access panels/controllers. The Hot List file shall be downloaded to the physical access control system components at least daily.

The system shall have the ability to receive and maintain the Hot List file so that it is up-to-date. At the agency's option, the system shall provide the capability to manually update the Hot List file.

3.3.1.9 Maintain Access Database

The physical access control system shall maintain a comprehensive database of information, including authorized access by individuals or groups to specific locations. This database must be able to be updated so that employees can be added or deleted when they are hired or terminated. The database shall be ODBC complaint, allowing the importing, exporting, and converting of database files from external database systems. The database shall provide maximum flexibility to interface with other unidentified systems.

The database shall be able to be updated across Wide Area Networks so that authorizations can be added or revoked remotely by a central office if so desired by an agency. Additionally, the system shall provide access capability for remote system diagnostics and remote system administration functions (with adequate password authorization required).

3.3.1.10 Manage Visitor Control

The physical access control system shall have the capability to maintain a visitor database. The operator shall have the ability to enter demographic data about the visitor into the temporary visitor database, assign temporary access privileges, and issue temporary access cards. The operator shall also be able to delete visitors from the temporary visitor database and deactivate cards. The physical access control system shall be able to recognize temporary visitor cards and route access requests to the visitor database for authorization. When maintaining a visitor database, the agency shall adhere to all relevant privacy laws.

The Smart Access ID contact chip shall be able to be read by any installed contact chip card reader. Therefore, at a minimum, demographic data stored on the chip on a visitor's card shall be able to be read at any chip-based access control reader. Optionally, the physical access control system shall be able to retrieve and upload to the visitor database demographic data maintained on the card's integrated circuit chip.

The design of the visitor database shall be flexible enough to allow it to be used as a back-up procedure in case an employee forgets his/her Smart Access Common ID Card. Employees could be issued temporary cards and tracked in the visitor database to allow physical access when they forget their own permanent card.

3.3.2 Physical Access Control Data

The access control transaction, at a minimum, shall capture a numeric identifier carried on the card and used to link to the cardholder record in a physical access control database. Individual agencies, at their discretion, shall provide additional data elements in the access control transaction. For example, to achieve interoperability across DoD agencies using magnetic stripe-based access systems, an agency may use the following data to remain in conformance with the SEIWG standard:

- **Agency Code –** this four digit code identifies the government agency issuing the credential;
- **System Code –** This four digit field identifies the system the card is enrolled in and is unique for each site;
- **Credential Number** - This six digit code encoded on the card by the issuing agency used as the card serial number (no duplicate numbers are available);
- **Credential Series –** this is a single digit field available to reflect major system changes;
- **Individual Credential Issue Number –** This single digit field, initially encoded as a "1", is to be incremented if a card is replaced due to loss or damage; and
- **Social Security Number –** This nine digit field contains the social security number of the credential holder.

At agency discretion, additional or other transaction elements may be used.

The specific data to be maintained in the physical access control database may vary by product and the implementation strategy of the agency. If the physical access control database is to be integrated with the centralized cardholder database, the data described in Section 1.1.1, as well as access privileges shall be included. In such a scenario, the database shall contain much of the same information that in the past was contained in the combined badge issuance/physical access control database. However, if the physical access control database is to be a separate database, more limited data shall be contained including, but not limited to:

- Name;
- Access System Numeric Identifier; and
- Access privileges.

Additionally, on the physical access control host server individual transaction/log records from the field devices and terminal inputs shall be maintained.

3.3.3 Physical Access Control System Performance

The physical access control system shall meet agency specific performance requirements. However, the following are considered to be common industry standards:

- Accept and process, at a minimum, five access requests, either from a local access panel/controller, or from an operator query, within one second;
- Process log-on transactions at the system host within 5 seconds as measured from the time the entry key is depressed after input of the password until a system acknowledgement is displayed on the operator's monitor;
- Process all operator entered commands within one second and update the appropriate transaction record on the database within two seconds;
- Process accesses to the card database for validation within 2 seconds to provide real-time response and action as a result of an access;
- Provide a system that shall have sufficient capacity to handle 150% of the expected peak hour transaction rate (access points and card swipes) over the communications network; and
- Provide system performance monitoring to measure actual system utilization, transaction processing, and response time.

The physical access control system shall meet a standard for hardware component uptime availability of 99.97% that shall be calculated as follows:

- Total # of covered components X 24 hours X # of days per month, including all weekends and holidays = Total available component hours per month. Allowable component downtime is calculated as allowable component downtime X .0003.

- Total available component hours per month X .9997 = Total component uptime availability required. Total component downtime is defined as the difference between the total available hours per month minus the total component uptime availability per month.

Uptime availability for a covered component is defined as the period during which the component, including all of its sub-components are performing in working order. The covered components shall include the host, local access panel/controllers, workstations, and communication devices.

The host shall meet a standard for host availability of 100%, assuming that in the event of the loss of host services the elapsed time to failover from primary to back-up host does not exceed the agreed upon failover interval. The components shall meet industry standards for Mean Time Between Failures (MTBF) and Mean Time to Repair (MTTR).

The physical access control system shall be easily expandable for future growth. Thus, it must accommodate a 50% growth in the number of access points, cardholders, and database without upgrading the software, host processors, or degrading system performance. The local access panels/controllers shall have 20% spare input/output capacity.

3.4 Logical Access Control Requirements

Agencies vary substantially in their current logical access control environments and capabilities. Where logical access control systems are in place, they are not integrated with the agency's badge issuance or physical access control systems nor is a common hardware token (card) device used for both physical and logical access control. At a minimum, there is a requirement to use the same hardware token, i.e., the Smart Access Common ID Card to support the visual identification (badge issuance), physical access control and logical access control functions. The ideal is to integrate the badge issuance and physical and logical access control functions through a common or shared agency card management system (refer to section 3.1).

3.4.1 Logical Access Control Functionality

Computer System Security generally encompasses three functions:

- **Data Security –** Data security schemes utilize mechanisms, such as data encryption, to protect information;
- **Authentication –** Authentication techniques are used to prove the identity of an individual and provide access; and
- **Access Control –** Access control techniques are used to manage and control an individual's privileges to access workstations, databases, host systems, and other networks.

Data Security is beyond the scope of the Smart Access Common ID Program. This Program focuses on the individual, i.e., specifically authentication of the individual's identity and control of the individual's access to computers, databases, and networks.

Although the technical implementation may vary, the basic functional capabilities of the logical access control function shall be standard across systems. This basic functionality includes:

- Enroll employees;
- Assign access privileges;
- Update privileges;
- Authenticate individuals;
- Conduct access control transactions;
- Track/audit access; and
- Generate access reports.

To the extent possible and depending on agency requirements, the logical access control software and functions shall be configured via point and click forms utilizing graphical user interfaces.

3.4.1.1 Enroll Employee

The employee must be enrolled into the logical access control database and the individual's logical access privileges must be authorized in the database. As described in section 3.3.1.1 within the Smart Access Common ID Card program, different agencies could adopt various card issuance strategies. Although some agencies may have a common office to enroll employees in both the physical and logical access control systems, the assumption here is that badge issuance and physical access control enrollment occurs through the building security department and logical access control enrollment occurs through the information technology department. Under this scenario, the cardholder's demographic information, photo, fingerprint or other biometric, if used, and physical access control privileges were captured and entered into the physical access control system. Any specified information has been written to the card, and a Smart Access Common ID Card has been issued to the individual. It should also be noted, that while all employees will have a requirement for a badge and some level of physical or building access, not all agency employees will have logical access privileges. Only those Smart Access Common ID cardholders with access privileges will be enrolled in the agency's logical access control system.

During enrollment in the logical access control system, the cardholder's privileges shall be written to the database and the agency specified authentication mechanism shall be loaded on to the Smart Access Common ID Card. The authentication mechanisms may include passwords, PINs, biometrics, or certificates.

3.4.1.2 Assign Access Privileges

The vendor shall provide logical access control software that allows the agency's designated logical access control administrator(s) to authorize logical access control privileges for employees. The cardholder's access control privileges shall be maintained in a relational database. The access control privileges may be individual or group based or a combination of group and individual, depending on the agency's requirements. The logical access control software shall also allow the agency's designated administrator(s) to update, change or delete access control privileges for an individual or a group. Other methods such as time of day access or day of week access control restrictions may also be required and supported by the privilege database.

3.4.1.3 Authenticate Cardholder Identity

Authentication of the individual cardholder's identity is the first step in granting network/computer access. Rigorous authentication techniques are necessary to ensure protection of agency systems. Generally authentication schemes are based on the following authentication criteria:

- Something the user KNOWS such as a password or personal identification number (PIN);
- Something the user POSSESSES such as an authentication token or smart card; and
- Something the user IS (i.e., a physical characteristic) such as fingerprint or a voice pattern.[29]

Logical access control authentication under the Smart Access Common ID Program shall be based on strong or two-factor authentication, i.e., authentication shall be based on a combination

[29] FIPS Publication 190, Op. Cit., p. 5.

of at least two of the above authentication criteria. The possession of the Smart Access Common ID Card and the agency designated token carried on the card is a required authentication factor. The other factor in the two-factor authentication scheme may be either a password/PIN (i.e., the smart card's PIN) or a biometric. If a digital certificate is carried on the Smart Access Common ID Card to support logical access control and other applications, the requirements specified in section 3.5, *PKI Service Requirements,* must be met.

There shall be a back-up mechanism (e.g., user ID, PIN or temporary card) established to enable an employee who has forgotten his/her ID card to be able to temporarily authenticate him/herself to the logical access control system.

3.4.1.4 Conduct Logical Access Control Transaction

All individuals requiring access to the agency systems shall be established or enrolled in the system. Access to workstations or computer devices, files, databases, programs, intranets, extranets, and Virtual Private Networks shall be based on the individual's access control privileges as authorized and established in the logical access control database. Before access is granted, the system must conduct an access verification transaction to check cardholder's access privilege in the database. Access shall be denied to individuals who do not hold privileges to access the workstation or computer devices, file, database, program or network they are attempting to access. The system must support a lock-out threshold for excessive invalid access attempts and must immediately block access by any cardholder or individual whose access privileges have been revoked.

3.4.1.5 Track/Audit Logical Access

The logical access control system shall have the capability to track and create an audit trail of all system access transactions conducted by an individual or a group. The system must include a method to secure this data and protect such records from modification, unauthorized access or destruction. The system shall record the following types of events: log on, log off, change of password, creation, deletion, opening and closing and access to files, programs, databases, and network, and program initiation actions. The system shall also record actions by the system administrator(s). At a minimum, for each event, the audit record shall identify: the date and time of the event, user, type of event, point of origin of the transaction event, the program, database or network to which access was directed, and the success or failure of the event. Depending on their requirements, agencies may specify additional data elements that must be captured for each event or transaction.

3.4.1.6 Logical Access Control Reporting

To support system administration functions, the logical access control system must provide the capability for creating reports on logical access transactions and events. The reporting requirements shall be specified by the agency and are expected to include requirements for ad hoc, query and standard reporting functionality.

3.4.2 Logical Access Control Data

The Smart Access Common ID Card itself shall contain the necessary digital certificates, attribute certificates (containing biometric templates), or passwords to authenticate the user to all the appropriate network, workstation, database, or application resources. The specific data elements retrieved from the card and presented in a logical access control transaction may vary depending on the implementation strategy of the selected logical access control application.

3.5 PKI Service Requirements

Recently, the United States Code was amended to mandate the electronic submission of information and the acceptance of electronic signatures. To assist in the implementation of this U.S. Code amendment, the Government Paperwork Elimination Act was passed as part of the Omnibus Appropriations Bill. The Government Paperwork Elimination Act directs the Director of the Office of Management and Budget to develop procedures for the use and acceptance of electronic signatures by Executive Agencies within 18 months. Furthermore, this Act sets a five-year deadline, in which time Executive Agencies must have implemented these procedures for use and acceptance of electronic signatures.

In order to use public key cryptography for identity authentication, encryption, and electronic signatures on a wide-scale, it shall be necessary to establish an infrastructure, commonly referred to as the Public Key Infrastructure (PKI), to support the generation and distribution of keys. Public key certificates can be used to authenticate the identity of the owner of a specific public key. A public key certificate is a digital document that, at a minimum, contains the name and public key of a user, signed by a Certificate Authority, a trusted third party who attests to the identity of the public key holder.

The architecture of a PKI characterizes the nature of the relationships between CAs that issue and verify each other's certificates. In such an environment, certificates may be chained to form a certification path. Trust is transferred via these certification paths in a PKI. A certification path is nothing more than a chain of certificate verifications in which the signature on the previous certificate is verified by the public key of the next certificate until a certificate is reached which is trusted by the verifier. This is usually the CA of the verifier.

CAs can certify each other in some systematic manner to form a PKI. A CA may be issued a certificate by another CA. Two CAs may issue each other certificates; this is known as *cross-certification*, and the pair together is a *cross-certificate*. Two alternative PKI architectures, based on these certificate validation chains, are described below:

- **Hierarchical –** Authorities are arranged hierarchically under a "root" CA that issues certificates to subordinate CAs. These CAs may in turn issue certificates to subordinate CAs, or to users. Every user knows the public key of the root CA, and any user's certificate may be verified by verifying the *certification path* that leads back to the root CA.

- **Network –** Independent CA's cross-certify each other, resulting in a general network of trust relationships between CAs. A user knows the public key of a CA near himself, generally the local CA that issued his certificate, and verifies certificates by verifying a certification path that leads back to that trusted CA.[30]

A hierarchical PKI architecture generally works best for government or military applications. In a network architecture, each CA issues a certificate to the other. Each can place trust in the certificates issued by the other without both being subordinate to a common CA. The network PKI architecture seems to be a better fit for the competitive marketplace.

The implementation of this infrastructure to support public key cryptography requires a defined set of services that must be provided by some entity. Agencies may opt to provide some portion of the services themselves, may designate another government agency to provide these services on their behalf, or may contract with a commercial entity independently or through this procurement to provide these services. Agencies may vary in their approach to PKI service delivery. Some agencies may opt to provide some services in-house and outsource the rest. Other agencies may choose to outsource all PKI services. Regardless of the delivery strategy chosen by an agency, the prescribed mandatory set of PKI services, described below, must be included in any PKI implementation. It is important to point out that any agency looking to implement a PKI should first review or create their Certificate Policy and Procedures.

3.5.1 PKI Functionality

Agency employees who have a need to securely authenticate their identity shall receive Smart Access Common ID Cards that contain a digital certificate after they have proven their identity to the designated entity functioning as a Registration Authority (RA). These certificates can then be used for identify authentication, access control, and signing.

Agencies may choose to implement their certificate programs somewhat differently. Typically, certificates shall be generated and maintained by an agency designated Certificate Authority which shall interact with one or more Registration Authorities. Alternatively, the agency may opt to act as its own CA or obtain the services of another government agency (e.g. the National Technical Information Service) to act as a CA on its behalf. Either the certificate applicant shall generate a public/private key pair or the RA or CA shall generate a key pair for the applicant. If the RA is the key generator, the RA shall then transmit the applicant's public key and identity information to the CA that shall issue the certificate. Otherwise, the CA shall generate the keys and the certificate. The certificate verifies that the applicant has established his/her identity to the satisfaction of the RA. When the certificate holder later attempts to access a system or sign a document, the respective application shall determine the identity of the certificate holder, validate his/her certificate with the appropriate CA, and then grant access or accept the signature as appropriate.

[30] Burr, William E., Nazario, Noel A., and Polk, W. Timothy, "A Proposed Federal PKI Using X.509 V3 Certificates, " Gaithersburg: National Institute of Standards and Technology, p. 3-5.

Although the entity designated as responsible for a particular PKI service may vary depending on the implementation scenario chosen by an individual agency, the functionality of the required services remains similar across different implementation strategies. The services needed to support a PKI implementation are described below.

The materials in Sections 3.5.1.1 to 3.5.3.4 are based on the General Services Administration's *Access Certificates for Electronic Services (ACES) Draft Request for Proposals (Solicitation Number TIBA 98003).*[31]

3.5.1.1 Enroll/Verify Employees/Generate Key Pairs

An agency designated entity (or the agency itself) shall act as the Registration Authority to register users and perform the identity proofing procedures. The employee shall provide the designated Registration Authority proof of his/her identity. The documents to be accepted as proof shall be at the agency's discretion. The RA shall perform the following functions:

- Inform the applicant that identity credentials shall be validated through the processes described by individual agencies;
- Obtain permission to verify the credentials from the applicant;
- Verify the identity of the applicant using the procedures prescribed by the individual agency;
- Register all applicants successfully identified; and
- Create, maintain, and protect from unauthorized access or disclosure such records as required to demonstrate how the identity of each registered applicant was established.

The identity verification process performed shall be stipulated by the individual agency. The specified data elements that shall form the basis of the verification process shall also be at the discretion of individual agencies. If the applicant passes the RA verification process, the RA shall notify the applicant of the successful completion of the verification process and record the following transaction audit data:

- Name of document presented for identity proofing;
- Issuing authority;
- Date of issuance;
- Date of expiration;
- All fields verified;
- Names of RA and CA;
- All transaction data;
- All associated error messages and codes;
- Date/time of transaction transmission; and
- Name (ID) of RA And CA process.

[31] *Access Certificates for Electronic Service (ACES): Draft Request For Proposals (RFP) – Solicitation Number TIBA 98003*, Op.Cit., p. C-11-32.

If the applicant fails to verify, the RA shall notify the applicant and provide all verification information to the applicant; at a minimum the RA shall:

- Indicate failure of registration verification process, including the success or failure of each field attempted to be verified;
- Inform the applicant of the requirements necessary to accomplish successful identity verification;
- Suspend or end the current application process;
- Record the transaction audit data:
  - Name of document presented for identity proofing;
  - Issuing authority;
  - Date of issuance;
  - Date of expiration;
  - All fields verified;
  - Fields that failed verification;
  - Status of current registration process (suspended or ended)
  - Names of RA and intended CA;
  - All transaction data;
  - All associated error messages and codes;
  - Date/time of transaction transmission; and
  - Name (ID) of RA and CA process.

If the RA generates the individual’s private key, it shall be generated on the Smart Access Common ID Card prior to distribution of the card or transmitted securely to the user. If it is to be transmitted, the private key shall be encrypted using the PKCS#5 Password –Based Encryption Standard (used to encrypt the private key when transferring them from one computer system to another), as well as the syntax prescribed in PKCS#8 Private Key Information Syntax Standard. The RA shall not retain any copies of the individual’s private key. If the cardholder generates the key, the corresponding public key shall be securely transmitted to the RA. After successful completion of key pair generation and identity proofing by the RA, the RA shall securely transmit a certificate request message to the CA over a mutually-authenticated link.

3.5.1.2 Issue Certificates/Generate Key Pair

The CA shall be responsible for the manufacture of certificates. Upon receipt of a valid certificate request message from a RA, the Certificate Authority shall perform the following functions:

- Verify the RA signature;
- Generate a CA-specific, unique certificate identifier;
- Generate a certificate;
- Indicate the applicant’s certificate as currently valid;

- Deliver the certificate to the individual in accordance with the delivery methodology required by the agency; and
- Record the following transaction audit data:
    - Names of RA and CA;
    - Copy of certificate;
    - Method of delivery to the applicant;
    - All transaction data;
    - All associated error messages and codes;
    - Date/time of transaction transmission; and
    - Name (ID) of RA and CA process.

At agency discretion, certificates could either be placed on the card at the time of card issuance or added at a future time. If the certificate generation is to be part of the card issuance process and the CA is responsible for key pair generation, the private key shall be generated on the Smart Access Common ID Card and the digital certificate shall be placed on the card prior to delivery of the card to the cardholder. If the RA or another party is responsible for key pair generation, the private key shall be generated on the card and remain on the card, the public key shall be transmitted to the CA, and the X.509 Certificate shall be securely transmitted to the point of card issuance to be loaded on the card prior to issuance. The specific process for key generation and certificate issuance may vary depending on the various scenarios adopted by individual agencies.

3.5.1.3 Maintain Certificate Repository/Certificate Policies

The CA shall be responsible for publishing the digital certificate in a repository. The CA shall maintain the certificate repository using the LDAP protocol and shall be responsible for ensuring the security of the repository. The CA shall promptly post certificates to the repository upon activation and suspension/revocation notices upon issuance. The CA shall maintain any relevant certificate policies in the repository. Additionally, the CA shall maintain a copy of its Certificate Practice Statement in the repository.

3.5.1.4 Validate Certificate Status

The CA shall be responsible for validating certificates it has issued. Validation functionality shall be performed through on-line validation protocols. At agency discretion, a particular agency/application may agree to accept certificates issued by other agencies (or the CA functioning on behalf of the agency). A certificate presented to the agency application shall be considered invalid until the issuing CA has notified the agency/application that the certificate is valid or suspended. Each agency/application shall request validation for every certificate presented and the appropriate CA shall complete the validation process in “real time”. Validity status shall be one of the following:

- Valid;
- Invalid; and
- Suspended.

The agency/application shall require the capability to direct each certificate to the appropriate CA for validation. Certificate Arbitrator Module (CAM) software shall be required to provide the capability to direct each certificate to the appropriate CA for validation. The CAM shall provide the capability to route certificates to the appropriate CA for validation. CA's wishing to participate in cross-validation of other agency certificates shall be required to create appropriate interfaces to the CAM. All CA's wishing to utilize the inter-agency CAM shall build interfaces to the CAM that conform to the "CA-side" CAM Application Programming Interfaces (APIs). Agencies wishing to present certificates for cross-validation shall be required to build interfaces to the CAM for their appropriate systems, in conformance with the "agency/application-side" CAM API. Only those agencies interested in processing certificates from other agencies may have a need for the CAM. The CAM shall perform the following processes:

- Process certificates for each CA within the same number of processing cycles;
- Verify that the presented certificate is issued by a currently qualified CA;
- Perform appropriate error processing for certificates that cannot be processed or is not issued by a currently qualified CA;
- Check that the presented certificate is within its lifetime limits and perform appropriate error handling if it is not;
- Determine the appropriate CA;
- Generate a certificate validation request message and digitally sign the request;
- Forward the certificate validation request to the appropriate CA via a mutually-authenticated link between the agency/application and the CA;
- Validate the certificate validation request response or store transaction data when no response is received; and
- Return certificate status and time/date of validation check to agency/application initiating the validation request.

Upon receipt of a Certificate Validation Request message from an agency/application CAM, the CA shall:

- Validate the certification validation request;
- Generate and return a signed certificate validation request response message via a mutually-authenticated link; and
- Record the following transaction audit data:
    - Individual certificate serial number;
    - Certificate status;
    - Agency/application certificate serial number;
    - All transaction data;
    - All associated error messages and codes;
    - Date/time of transaction transmission; and
    - Name (ID) of RA and CA process.

At agency discretion, other certificate validation procedures may be arranged with the designated CA.

3.5.1.5 Revoke Certificates

Certificates may become invalid (e.g., due to certificate holder's suspicion of loss or compromise of certificate). All certificate holders may request that their certificate(s) be revoked. The CA shall be able to immediately change the status of the appropriate certificate to be suspended. After the CA has completed identity proofing, the status of the certificate shall be changed to invalid or valid, depending upon the results of the identity proofing.

The CA shall be able to revoke certificates as follows:

- The CA shall provide on-demand certificate revocation, initiated by the registered holder of a certificate issued by the CA, only after repeating the proofing process appropriate for the certificate to be revoked;
- The CA shall provide for emergency revocation from registered agencies/applications in a streamlined process to protect the agency/application and its data in the event of compromise of its key(s);
- The CA shall revoke only certificates it has issued;
- The CA shall record the following transaction audit data:
  - Date/time;
  - RA and/or CA name;
  - Certificate policy OID;
  - Reason code;
  - Certificate serial number; and
  - All associated proofing, revocation, and transaction data.

3.5.1.6 Suspend Certificates

When a CA has received a request for certificate revocation, the CA shall:

- Immediately change the certificate status to "suspended";
- Complete identity proofing of the individual requesting the certificate revocation in accordance with the agency's prescribed procedures for identity proofing;
- Change the status of the certificate to invalid or valid, depending on the results of the identity proofing process; and
- Record the following transaction audit data:
  - Date/time;
  - RA and/or CA name;
  - Applicant's common name;
  - Certificate policy OID;
  - Status of certificate at end of suspension;
  - Reason code;

  - Certificate serial number; and
  - All associated proofing, revocation, and transaction data.

3.5.1.7 Renew Certificates

Prior to the scheduled expiration of the operational period of a Certificate, the subscriber may request the renewal of a currently valid certificate, provided the certificate has not been suspended or revoked. Such a request shall be made electronically via a digitally signed message based on the key pair of the certificate being renewed. The CA shall be able to accept Certificate Renewal Requests from its certificate holders any time within the certificate's lifetime, provided the certificate has not been revoked or suspended. Suspended, revoked, or expired certificates shall not be renewed. The CA shall notify certificate holders of the requirement to renew no later than 90 days prior to the certificate expiration date. The CA, except where the common name and/or key pair are changed shall process certificate renewals. In the event subject information and/or key pair are changed, a request for a new certificate shall be required. If the subject information has changed, the CA shall perform the specified identity proofing. The CA or RA shall re-authenticate applicants without a valid certificate and issue a new certificate.

The CA shall accept Certificate Renewal Requests in accordance with the agency's Certificate Policy and perform the following procedures:

- The CA shall verify that the certificate has not been revoked or suspended, and that the common name and key pairs have not been changed;
- The individual's current certificate shall be used to authenticate the individual to the CA for the certificate renewal process; and
- The CA shall record the following transaction audit data:
  - Certificate serial number;
  - Certificate common name;
  - Certificate policy OID;
  - New validation dates;
  - Date/time of transaction;
  - Name (ID) of CA process; and
  - All associated transaction data.

3.5.1.8 Perform Certificate Audit/Maintain Certificate Records

The CA shall maintain transaction audit data for all transactions related to the registration, issuance, validation, revocation, suspension, and renewal of certificates. The CA shall retain and protect from unauthorized access or disclosure the data listed below related to certificate issuance, certificate validations and transaction data, certificate renewal, and/or certificate revocation/suspension:

- Copy of certificate;
- Certificate identifier;
- Certificate common name;

- Date/time of action;
- Type of action (e.g., issue, renewal, revocation, suspension);
- Identity proofing data fields from certificate issued; and
- If revocation, reason code.

Certificate audit data shall be maintained in a secure environment. The archive of key and certificate data shall be retained for at least 30 years. If this is not acceptable to individual agencies, the time period for which such data shall be maintained shall be modified at the discretion of the agency. Each CA and RA shall provide Government-authorized representatives ad hoc access to all audit data relating to an agency or agency application.

3.5.2 Certificate Data

As stipulated in Section 2.3.3.5, the data maintained in the certificate shall conform to the X.509 Version 3 format A recommended certificate format and suggested naming conventions are included in Appendix B.

3.5.3 Performance Characteristics

The RA and/or CA shall meet or exceed performance standards in the following areas:

- Hours of operation;
- Availability of services;
- Response time for services; and
- Accuracy.

3.5.3.1 Hours of Operation

The RA and/or CA shall operation the following services 24 hours per day, seven days per week including Federal holidays:

- Certificate application and renewal services;
- Certificate validation services;
- Certificate suspension/revocation services;
- Emergency certificate revocation services; and
- Customer service center.

3.5.3.2 Availability of Services

All of the RA and/or CA services and products described in the above sections shall be in operation and available for use, during the required hours of operation, not less than 99.5 percent of the time.

3.5.3.3 Response Time for Services

The RA and/or CA shall not exceed the minimum response times indicated in the table below:[32]

[32] Ibid., p. C-30.

Transaction/Process	Response	Constraints
Identity proofing	3 days	>= 95% of all transactions within response; max of 5 days
Identify proofing failure notice	3 days	>= 95% of all transactions within response; max of 5 days
Certificate delivery, from completion of identity proofing	3 days	>= 95% of all transactions within response; max of 5 days
Certificate Validation, from receipt of request	30 seconds	>= 95% of all transactions within response; max of 2 minutes
Renewal of a certificate	10 min.	>= 95% of all transactions within response; max of 24 hours
Individual Certificate Revocation Request (CRR) message	3 days	>= 95% of all transactions within response; max of 5 days
Suspension of Certificate following CRR message	10 min.	>= 95% of all transactions within response; max of 1 hour
Emergency CRR message	10 min	>= 95% of all transactions within response; max of 1 hour

The performance requirements suggested above may be adjusted to meet individual agency requirements.

3.5.3.4 Accuracy

Error rates for user registration, certificate issuance, certificate validations, certificate suspension/revocations, and certificate renewals, as well as the probability of message loss, shall be in accordance with best commercial practices.

3.6 Biometric Services

A biometric will be mandatory for the Smart Access Common ID Card, so that any authorized Smart Access Common ID Card vendor team shall be required to provide at least one biometric capability. Agencies shall have the option of selecting from the offered biometrics for the Smart Access Common ID Card program. Each of the biometric types described below has it own set of strengths and weaknesses. Depending on the requirements, circumstances, and environment of a given agency, certain biometrics will be better suited than others for that particular agency. Although there are many different types of biometrics in use today, only the following commercially-available biometrics are included within the scope of the Smart Access Common ID Card program:

- **Fingerprint Scan** – The fingerprint is one of the most widely used biometrics in the government today. It is currently the mandated biometric for the Department of Defense. Fingerprints are well known to the general public, having been used to verify identity for a number of years. Use of a fingerprint requires that the user place one or more fingers on a platen on the fingerprint scanner. Different technologies are used by scanners to capture fingerprints and convert them to templates that can be used for verification comparisons. One method analyzes the position of minutiae, which are the end points and junctions of ridges. Yet another method regards the fingerprint image as a pattern; the whorls, loops and tilts are digitized to make a visual comparison with the offered print. The difference in methodologies for capturing fingerprints and converting them to templates makes it difficult to develop a standardized fingerprint template.

- **Hand Geometry –** Hand geometry is currently being used within the government in several agencies including the Department of Energy and the Department of State. Hand geometry systems use optical systems to map key geometrical features of the topography of a hand to verify an individual's identity. Hand geometry technology uses a number of different measurements to create the template. These readings may include measuring finger length, skin translucency, hand thickness, and palm shape. Different products use diverse methodologies to construct the hand geometry template, so there is currently no standard template that can be used for smart cards. Live scans of the hand are compared against the template to verify a person's identity.

- **Facial Recognition –** Facial recognition is currently being used by several state motor vehicle departments to provide identify authentication in the issuing of drivers licenses. Facial recognition is based upon comparison of the characteristics of a live scan of a face against a stored template of facial characteristics. Various technologies may be used to perform facial recognition. Some products utilize off-the-shelf video/digital cameras. Such products employ algorithms to create a set of numbers related to the face rather than the facial image itself. One method uses spatial measurement, recording such distances as the center of the eye to the bottom of the ear, to the tip of the chin, and to the high cheek feature. Another method uses two cameras to record a stereo view of the face. This method evaluates the entire face, not just key features. Other products use infrared technology. Because the technology for creating facial templates varies from product to product, there is no standard facial recognition template.

- **Iris Scan -** The iris of the eye is a mathematically unique feature of the human body. Each iris is composed of a unique visible structure, which features a complex combination of corona, pits, filaments, crypts, striations, radial furrows, etc. It is this structure and pattern that is imaged and encoded in the iris template. The iris has limited genetic penetrance, which ensures that even identical twins have iris patterns as distinct in their mathematical detail as those of unrelated persons. To capture an iris scan, a video/digital camera takes a picture that locates the eye and iris. The boundaries of the pupil and limbus are defined, eyelid occlusion and specular refection are discounted and the quality of image focus is determined for processing. The iris pattern is processed and encoded into a template that is stored on a smart card. It is then compared against the live iris scan image obtained by having the user merely look into a reader.

- **Voice Recognition** - Voice verification is possible because every person has a unique set of voice characteristics and speech patterns. Voice verification extracts specific and unique features from a person's speech, such as pitch, tone, cadence, harmonic level and vibrations in the larynx and stores and uses them to differentiate that person's voice from other voices. All voice recognition systems require speech samples from each user to associate with the user's profile or account. A person using a voice verification system begins by claiming to be an enrolled user. This is generally accomplished by speaking or otherwise inputting an identification code. The spoken input is compared with a stored sample of the enrolled user's speech. This stored sample is called a voice print. If the two samples, voice print and spoken input match, then the person is accepted. If they do not match, the person is rejected and denied access. Voice is a very convenient verification system for use in telephonic transactions. Voice verification can greatly enhance security for dial-up computer links and terminal access so it is particularly popular for logical access control applications.

It is assumed that some biometrics will be adopted by a majority of participating agencies, while others will be less commonly used. Although agencies may opt to use any of the biometrics within the scope of the Smart Access Common ID project, agencies choosing common biometrics are more likely to realize economies of scale.

Although the technology varies from biometric to biometric, all biometrics within the scope of the Smart Access Common ID Card program share similar functionality. Because the Smart Access Common ID Card program shall focus on verification rather than identification, the following generic functions shall be required for each of these biometrics:

- Enrollment;
- Capture;
- Translation; and
- Verification.

3.6.1 Biometric Functionality

Agency employees who have a need to securely authenticate their identity shall receive Smart Access Common ID Cards that have an attribute certificate (referred to in other parts of the document as a "biometric certificate") containing their biometric template, after they have confirmed their identity to the designated entity functioning as an Attribute Authority. These certificates can then be used for identity authentication and/or access control. The biometric in the attribute certificate shall be used for authenticating the cardholder's identity. It potentially could be used to grant access to private keys on the card, to physical facilities, or to computer/network resources.

The Smart Access Common ID Card program will utilize the biometric verification process (one to one matching) rather than the biometric authentication process (one to many matching). A live biomeric scan shall be captured at the initial enrollment of the cardholder. This biometric shall be translated into a template that shall be stored on the card. When the cardholder wishes to verify his/her identity, a live scan of the biometric is taken, translated into a template, and compared against the existing template on the card. The template on the card shall be in the form of an attribute certificate that has been signed by an Attribute Authority.

The services needed to support a biometric implementation are described below.

3.6.1.1 Enrollment

An employee applicant shall visit in person the designated card enrollment site and provide a "live" biometric scan. The biometric image capture device shall be linked to the imaging workstation used to perform the card enrollment process.

The biometric scanner, either by itself or in concert with the imaging workstation, must be capable of periodically performing automatic self-diagnostic and calibration to ensure that peak image quality is maintained.

The enrollment process may vary depending on the implementation strategy of an agency. A typical strategy description follows. Once the enrollment livescan biometric image is captured, it shall be processed into a biometric template that shall be stored on the Smart Access ID Card within an attribute certificate. The biometric template, the Smart Access Common ID Card's serial number, the subject's name (or public key certificate's serial number if preferred by an agency), and the user's authentication information shall be sent to the Attribute Authority. The Attribute Authority shall create the X.509 formatted attribute certificates. The biometric certificate, containing the enrollment biometric template, shall be returned to the enrollment station and placed in the Smart Access Common ID Card.

At an agency's discretion, the procedures and entities responsible for each of the procedures may vary from the description provided above. For example, the enrollment biometric scan could be converted to a template that is, in turn, transmitted to a Bulk Card Personalization Center. Such a Center could generate key pairs, send relevant information and public keys to a CA to obtain digital certificates, send the biometric template and other relevant information to an Attribute Authority to obtain attribute certificates, and load the card with data and certificates. Once the cards are completed, having had the required cardholder information, digital, and attribute certificates loaded to the card, the card shall be returned to an agency on-site card distribution point for issuance to the employee.

Individual agencies may choose whether or not to maintain copies of enrollment templates on the central card management database. Agencies opting to store the enrollment template in the cardholder database must ensure that the template is securely transmitted to the central database. This information may be accompanied by demographic data and other data as required by the individual agency.

3.6.1.2 Capture

Once the user is enrolled, the biometric shall be used to verify the user's identity. When the user identity needs to be verified, a livescan of the user's biometric image shall be acquired from the biometric scanner. At this point in the process, the raw biometric data are captured that shall in turn be processed to create the livescan template used in the template comparison. The biometric capture device shall have the following:

- Capability to prompt the user to place his/her physical attribute for scanning;
- Capability to detect common problems such as improper physical attribute placement and provide feedback to the user for correcting the problem and repeating the verification process; and
- Capability to provide clear, interactive instructions for use of the system functions.

Biometric products capture varying biometric characteristics and use different algorithms to perform the biometric verification process. Processing parameters contained in the biometric certificate shall help define what parameters shall be considered in capturing the live biometric image. These processing parameters, in turn, shall be input to the processes in the next step which are used to create a livescan biometric template to compare against the biometric template found in the attribute certificate. Such parameters may include the following:

- **Minimal Acceptable Quality –** A minimum quality that the sample must have to be accepted for further processing (e.g., this may relieve the need for users with a scarred finger to reenter the fingerprint sample several times for verification); and
- **Number Of Samples –** The number of samples that should be taken of the user which meet the minimum acceptable quality threshold (e.g., this will help users with poor biometric characteristics avoid reentering livescan samples several times).

3.6.1.3 Translation

The analog information obtained from the biometric capture device must be converted to a digital representation to be able to be used by the matching algorithm. The raw biometric image data, together with the processing parameters contained in the biometric certificate, shall be fed to the biometric processing function that converts the livescan image to a livescan biometric template. The processing parameters contained in the biometric certificate shall be used by different products to control the processing that transforms the live image into a live template to be used by the verification function.

3.6.1.4 Verification

Once the livescan biometric template has been created and the signature on the biometric certificate has been verified to detect alteration and prove the validity of the biometric template, the verification processing can occur. The livescan biometric template, the enrollment biometric template from the biometric certificate, and the matching algorithm parameters from the biometric certificate shall be fed into the matching algorithm to verify the user. The biometric matching algorithm shall take the two templates and compare them for similarities.

The output of the matching function shall be a matching score that represents the amount of similarity found between the two templates. A livescan typically does not exactly match the user's stored template. Since there are almost always variations in biometric measurements, the systems can not require an exact match between the user's original enrollment template and a current biometric. Instead, the livescan template is considered valid if it is within a certain statistical range of values. Consequently, the output of the matching algorithm, the matching score, shall indicate whether or not the matching is within required range of values. If the result falls into an "acceptable" range, an affirmative response shall be given; if the result falls into an "unacceptable" range, a negative response shall be given. Matching parameters found in the attribute certificate may be supplied to provide the matching algorithm specific information to personalize the matching process for the individual. An example of matching parameters may be:

- Mini**mal Acceptable Matching Threshold –** This may be used to adjust the sensitivity of the matching process for an individual with poor biometric characteristics; and
- **Template Identifier –** This may be used to distinguish the biometric template in question from others found in the certificate (e.g., it may be used to distinguish which biometric the template represents if there are multiple templates on a card).

The workstation or physical access device upon which the biometric verification function is performed shall be capable of automatically receiving the verification results and displaying them to the user.

3.6.2 Biometric Performance Requirements

The performance of the biometric subsystem of the Smart Access Common ID Card platform is critical to the card's acceptance by the user community. Although convenience is important, the biometric system's accuracy and speed of throughput is also key to acceptance of a biometric in this employee card program.

3.6.2.1 Accuracy (False Acceptance Rates/False Rejection Rates)

The False Acceptance Rate (FAR) is the rate at which an unauthorized individual is recognized as a valid user. The False Rejection Rate is the rate at which a valid user is rejected by the system. Systems can be adjusted to increase or decrease each of these factors. The system administrators must balance the false acceptances versus the false rejects to ensure adequate security while remaining cognizant of user convenience.

The products shall specify the procedures used to determine False Acceptance and False Rejection Rates. It is important that uniform procedures be used to test FAR/FRR so that the results are comparable across products.

3.6.2.2 Throughput Rate

The combination of acquisition and processing times vary among the devices. Additionally, false rejections, which require human intervention, may further slow usage of the device and the resulting mean throughput rate. Depending upon the application, throughput rates may be of significant importance. The biometric verification system must be able to scan an individual's biometric, perform a verification match against the card-based biometric template, and display the results in one (1) second or less.

3.6.2.3 Environmental Requirements

Biometric capture devices shall be able to be adapted to the environmental conditions needed for the applications in which the biometric shall be used. For example, biometric capture devices associated with a physical access control system shall be able to withstand extremes of temperature associated with an outside reader.

3.6.3 Biometric Data

The biometric template on the Smart Access Common ID Card shall be contained in the biometric certificate. The format of the biometric certificate containing the biometric template shall conform to Appendix D of the *Guidelines for Placing Biometrics in Smartcards.* Because there are many different processes capable of performing biometric verification, the data structure used must be flexible enough to hold varying formats of data, as well as information needed for correct processing. Thus, the data structure must be able to contain the biometric template, as well as optional fields to provide processing parameters and matching algorithm-specific information.

Diversity in product operation and approach is responsible for the lack of standardization of the data that comprises the biometric template. Because individual products perform the processes for scanning, creation, and matching of templates differently, no standard data set exists even within a particular biometric type. Although efforts to create a standard biometric template within some biometric types (particularly fingerprinting) are currently ongoing, it may be a long time before such a standard template is achieved for any biometric technology. Once such standard templates are available, it is the intention of the Smart Access Common ID Card program to conform to such standards. However, there is no possibility of ever achieving a standardized template across all biometric types.

3.7 Reporting

The agency needs the compilation and summarization of data on card transactions and monthly reports for the participating offices. The agency shall require strategies for reporting that provide the most efficient and cost effective combination of raw data extract and/or standard report formats.

The agency shall require four categories of reports: Audit, Program Management, Security and Fraud, and System Performance:

- **Audit Reports**: These are reports providing data necessary to monitor, reconcile, and audit system processing and reconciliation;

- **Program Management Reports**: These are reports, such as program participation reports, that provide information that will be useful in managing and adapting program services;
- **System Performance Reports**: These reports are used to monitor the operation and performance of the Smart Access Common ID Card platform systems; and
- **System Fraud and Security Reports**: These reports provide information that assist in the detection of fraud and ensure system security. Data provided includes information such as:
  - Attempts (by location) to log on to the system using invalid passwords;
  - Electronic purse account balances that exceed established tolerance for differences between the reported purse value and the derived purse value;
  - Cards reported lost or stolen; and
  - Disputed or erroneous transactions.

The agency shall identify specific reporting requirements.

4 OPTIONAL FUNCTIONAL REQUIREMENTS

At agency discretion, additional options and capabilities shall be made available for the Smart Access Common ID platform. Such options and capabilities shall be made available at the discretion of the vendor team(s). While the vendor team(s) shall be required to provide all mandatory requirements, the vendor team(s) shall have the authority to decide whether or not to provide optional requirements. Should an agency desire an optional capability for its Smart Access Common ID Card, the agency shall be able to procure such a capability from either the vendor team who has chosen to provide such an optional capability or through an additional service provider who has been authorized to provide the desired capability.

4.1 Basic Identification

Although the mandatory data elements that typically shall be included in the Smart Access Common ID Card have been stipulated in Section 3.2.2, many agencies may opt to add additional elements or to remove certain elements provided on the card. While agencies shall provide the capability to authenticate an individual cardholder’s identity through entry and verification of a PIN, password, or biometric, not all agencies will opt to use the card as a component of a physical access control system. At the most basic level, the card will provide a physical “flash” pass that verifies the cardholder’s identity through a digitized photograph on the face of the card. The chip on the card may be programmed to contain demographic data that can be read by a card access device. At an agency’s discretion, identification functionality may be initially limited to basic identification without being linked to other access control applications while an agency prepares to take full advantage of the value that a multi-application smart card provides.

4.1.1 Physical appearance of card

Although GSA recognizes the desirability of a common “look and feel” to a Federal governmentwide identification card, GSA also understands that individual agencies may have specialized requirements for the physical appearance of the card. Because of these specialized requirements, as well as prior investments in legacy card systems, agreement on a single physical standard may be problematic for some agencies. Consequently, as long as agencies conform to the technical standards specified in the appropriate sections above, agencies may optionally determine the physical appearance of the card. While some limitations may occur through conformance to these technical standards (e.g., the location of the contact chip interface is specified by the 7816 standard and may preclude placement of certain data elements in a particular location), it is the intent of the GSA to allow individual agencies to control the color, data placement, and format of the “real estate” on the smart card. To the extent that common characteristics or a governmentwide logo or physical appearance can be agreed upon in the future, GSA supports the effort to achieve standardization.

4.2 Property Management

An application related to physical access control is property management. A substantial amount of time is currently expended on obtaining and presenting property passes when an employee wishes to take a laptop computer or other agency assets out of the building. Assets that must be managed include:

- Computer equipment;
- Telephones/telecommunication equipment;
- Credentials;
- Arms;
- Automobiles; and
- Other agency specific equipment.

Currently, the employee must obtain a paper property pass that specifies the characteristics of the equipment in his/her possession. Completing the paper property passes is often a time consuming task. Guards must verify the property passes each time the employee enters or exits the building. The passes are generally issued for short periods of time and must be frequently renewed, requiring substantial paperwork. When surveyed, agency personnel indicated that a substantial amount of time can be spent on issuing, updating, and checking property passes. Furthermore, employees may need to bring equipment in and out of guest agency buildings.

Several surveyed agencies have special parking facilities for fleet vehicles. Only those employees authorized to use agency vehicles may access these parking facilities. Authorized entry and exit of fleet vehicles needs to be verified. The concept of a property pass could be extended for controlling access to these fleet vehicles.

The sections below describe the processes and data that shall be implemented for a card-based property management application.

4.2.1 Property Management Functionality

A property management application could be implemented in several ways:

- **Chip-Based Property Management –** A chip-based application would provide the capability to enter, update, and delete asset information from the employee's card. This asset information could then be manually read and verified by a guard when the employee enters or exits a building; and

- **Tag-Based Inventory Control –** Radio frequency (RF) tags could be placed in assets and read automatically when the employee passes through a portal.

The sections below detail the functionality associated with these property management approaches.

4.2.1.1 Chip-Based Property Pass

A chip-based property pass application shall include the following functions:

- **Create Property Pass –** This function shall be used to link an asset (e.g., laptop computer, telephone, credential, gun, automobile, etc.) to a specific employee. Identifying and descriptive information about the asset, the time frame during which the property pass is active, and any specialized access control privileges relating to the asset (e.g., SCIF facility use only, home use allowed, etc.) shall be entered on the chip, as well as transmitted to the central cardholder database;

- **Maintain Property Pass –** This function shall be used to update information about an asset linked to a specific employee. Data about the asset, the property pass period of validity, or access privileges may be updated or deleted from the chip on the Smart Access Common ID Card using this function. Additional assets also may be added or deleted from the employee's card using this function;

- **View Property Pass –** This function shall be used to view the asset information on the employee's card. When an employee enters or exits a building, the guard shall ask the employee to insert his/her card to verify that he/she is authorized to bring in or take out designated assets. The guard shall then compare the identifying information on the terminal display with the information on the asset under examination to verify that the employee is authorized to have this asset. A similar function could be used in parking facilities with automobiles; and

- **Generate Property Pass Reports –** This function shall be used to generate reports on the use of property passes. Managers could generate inventory reports as well as reports on when assets were entering/leaving the building.

Since the Smart Access Common ID Card shall be able to be read in agencies other than the employee's home agency, an employee wishing to take an asset from his/her agency's building to another agency's building shall be authorized to do so using the information on the card. The guard staff in the receiving agency shall read the employee's card to verify that that employee is authorized to have the property coming into or going out of the receiving agency's building.

4.2.1.2 Tag-Based Inventory Control

A tag-based inventory control system shall automate the function performed by the guard in the application described above. In this application, a radio frequency tag shall be placed in any equipment or vehicle to be assigned to an employee. The tag numbers shall be linked with the appropriate employee in the physical access control system database. When an employee walks through a portal, the RF tag in the asset shall be read and verified against the physical access control database. If the employee is authorized to have the asset and to enter/exit the facility, access shall be granted. Otherwise, the system shall either sound an alarm or deny access. This application shall include the following functions:

- **Enroll Employee –** This function shall be used to link the asset with the employee in the physical access control database. If the employee is not already in the database, the employee shall be added to the physical access control system database. Each asset belonging to the employee shall be linked with the employee in this database;

- **Assign Access Privileges –** This function shall be used to set the access privileges. The access privileges/restrictions associated with each controlled employee asset shall be added to the physical access control database;

- **Conduct Access Control Transaction –** When an employee walks through a portal, the portal shall read the RF tag of any asset in the employee’s possession, route the transaction to the physical access control database, perform a search for the asset number in the database, and retrieve the appropriate access privileges;

- **Authorize Access –** Once the access privileges associated with an asset have been verified in the physical access control database, a transaction shall be sent to the access control devices. If the employee is authorized to have the asset, access shall be authorized and the gate/turnstile/lock shall permit entry/egress. If the employee is not authorized to have the asset, an alarm shall be sounded or the access device shall be blocked;

- **Update Privileges –** This function shall be used to update information about an asset linked to a specific employee. Data about the asset, the property pass period of validity, or access privileges may be updated or deleted from the physical access control system using this function;

- **Track/Audit Accesses –** This function shall be used to track what assets have been associated with what physical access events. Each time an employee enters or exits a facility with a particular asset(s), the access transaction shall be logged. This access transaction log could be searched to provide audit information as required;

- **Generate Access Reports –** This function shall be used to generate both standard and ad hoc reports. Reports could be generated that provide the date, time, and/or location of access events by a given employee with a given asset; and

- **Maintain Access Database –** This function shall be used to maintain the asset information associated with the physical access control database. Assets shall be added, deleted, or modified through this function.

4.2.2 Property Management Data

The following data shall be included on the chip for each asset assigned to an employee through this property management application:

- Asset identification number;
- Asset description;
- Asset type code;

- Asset license number (associated with vehicles only);
- Date of asset issuance;
- Date of property pass issue;
- Date of property pass expiration;
- Asset restrictions; and
- Asset access privileges.

4.3 Optional Physical Access Control Functionality

Although most physical access control functions shall be provided as mandatory services, certain capabilities may be considered optional as they will be required only by those agencies with high level security needs. The sections below describe the functionality associated with these physical access control options.

4.3.1 Exchange of Clearance Information Application

A substantial amount of time is expended exchanging clearance information between agencies for employees who must attend meetings or visit other agency facilities. While the intelligence community and military agencies are most likely to pass clearance information among themselves, a small percentage of employees from the civilian agencies must also occasionally exchange clearance information when visiting other facilities. Members of the intelligence and military communities who routinely pass clearance information among themselves are already linked through an on-line system that allows clearance information to be distributed through networked servers. Such a solution works very well in this closed environment in which agencies have established both inter-agency agreements and the technical capabilities to exchange clearance information with known partners. However, when clearance information needs to be exchanged in a more open and less routine environment, the transfer of such information becomes more problematic. In this scenario, an employee may be from an agency that does not have pre-established agreements or technology enabled links with the receiving agency. Because clearance transactions need not be exchanged routinely, the cost of creating on-line links between a multitude of agencies would be prohibitive. In this situation, the use of the Smart Access Common ID Card as a portable carrier of clearance information may prove to be the least expensive option to allow such information to be exchanged securely.

In one scenario, the designated Security Officer of the home agency would load, date, and digitally sign clearance information on the employee’s card. At the receiving agency, the guard would verify the Security Officer’s digital signature, read the clearance information, and match the information with a visitor request generated by the receiving agency employee. If all of these validations were successful, the visiting employee would be granted access. At the agency’s option, the data on the chip could either be used to create a temporary visitor’s badge or be uploaded to the physical access control database so that the visiting employee’s card could be activated to work in the receiving agency’s system.

This same functionality could be adapted for use of non-employees (i.e., contractors) who must visit government facilities on a routine basis.

4.3.1.1 Exchange of Clearance Information Functionality

The clearance information application shall provide the following functions:

- **Create Clearance Record –** This function shall allow clearance information to be added and dated on the chip;

- **Update Clearance Record –** This function shall allow clearance information to be added, modified, or deleted from the chip;

- **Certify Clearance Record** - This function shall allow the designated individual to digitally sign the clearance record, certifying that the data is correct and up-to-date. This function would allow the Security Officer both to generate a digital signature and to load his/her digital certificate on the card;

- **View Clearance Record –** This function shall allow the clearance record to be viewed by an authorized individual;

- **Verify Digital Signature –** This function shall allow the digital signature to be validated by an authorized individual;

- **Match Clearance Record to Visitor Request –** This function shall retrieve the visitor request and clearance information from the card and use this information to perform a verification match;

- **Upload Demographic Information –** This function shall provide the capability to retrieve relevant demographic information from the chip card, format the upload file, and upload the file to a visitor or a physical access control database; and

- **Delete Clearance Record/Certificate –** This function shall provide the capability to delete both the Clearance Record and the digital certificate of the signing Security Officer.

4.3.1.2 Exchange of Clearance Information Data

The Exchange of Clearance Information shall include the following data:

- Clearance type;
- Clearance status;
- Clearance issuance date;
- Clearance expiration date;
- Date of last investigation;
- Digital signature of transaction; and
- Security Officer’s digital certificate (see section 3.5.2).

At their discretion, agencies could use a clearance certificate for this functionality, following the ITU X.520 standard as a basis for a clearance attribute.

4.3.2 Integration With Other Systems

Some agencies may opt for more extensive functionality from their physical access control systems. These agencies shall incorporate a variety of highly sophisticated facility protection capabilities into their systems or build interfaces to related systems:

- **Alarm Monitoring System –** The physical access control system shall be able to be linked with an alarm or an intrusion detection system. An alarm monitoring and integrated color graphics program shall permit users to quickly and efficiently respond to incoming alarms. The system provides the capability to assign priorities to each alarm input. Higher priority alarms take precedence over lower priority events to insure that critical alarms are handled first. This software shall display alarm messages in priority order and time sequence and display messages to assist in operator response. Incoming alarms shall be displayed as flashing color alarm icons on detailed, user-designated facility maps. Colors can be assigned to each alarm condition. The system shall have the capability to enter text to be displayed each time an alarm occurs. This capability can provide guard instructions or emergency contingency plans. Furthermore, there shall be an operator response field for incident resolution logging. The system administrator shall have the ability to automatically redirect alarm reporting from any workstation to another workstation location for processing when operators fail to respond or move to another location. Alarm events shall have the ability to automatically trigger other equipment such as audio switchers, lighting, annunciators, and Closed Circuit TV system switchers. Suppression and activation of alarm points in the system shall be able to be manually controlled or automatically controlled through the use of system time zones. Global or local alarm masking shall be able to be performed either by the operator, cardholder, or both;

- **Closed Circuit Television Interface System –** An agency shall be able to link its physical access control system with a CC TV system, thereby allowing television cameras to be automatically focused on entrances in which an unauthorized access attempt sets off an electronic signal read by the CCTV system. The CCTV interface software shall allow users to define relationships between alarm points and CCTV camera call-up. Video switchers shall be integrated with the access control system through a serial RS-232 connection;

- **Alarm Paging Interface System –** To better manage guard coverage, the physical access control system shall be able to work hand-in-hand with a radio paging system such that an unauthorized access attempt can trigger a page to a guard patrolling more than one entrance. The system shall support the transmission of any alarm text messages generated by the physical access control system to any PET compliant radio paging base station. The base station then shall be able to transmit these text messages to an alphanumeric pager;

- **Guard Tour System –** The physical access control system shall be able to be linked with guard tour systems so that fewer guards can be used on a rotating basis to control multiple entrances. This optional capability shall provide the ability to enter on-line event messages to track guard progress through checkpoints. This system shall have the capability to generate historical reports to provide detail on past guard tour activity;

- **Elevator Control System –** This system shall provide the capability to restrict access to specified floors during designated time periods. It shall provide the ability to generate audit trail reports on floor access granted or denied through card reader controlled elevators;

- **Sensitive Compartmentalized Information Facility (SCIF) System –** This system provides the capability to set up special card access and alarm monitoring-related scenarios that meet the unique requirements of a SCIF;

- **Area Loading/Two Man Rule System –** This system requires that the card be used both for entry and exiting of a designated security area. It shall provide the capability to keep track of the number of valid cardholders who enter a designated security area, confirm the number of individuals in a security area at any time, define the maximum number of individuals who may occupy the designated area, and restrict access to the area when the maximum number is reached. The system also shall be able to reduce the occupancy count each time a cardholder exits a designated security area. The software shall also provide the capability to enforce that no less than two valid cardholders can be present in the designated area at any given time; and

- **Biometric Access System –** Biometric systems that perform the biometric verification function shall be incorporated into the physical control access system. The cardholder shall be verified by comparison of a live scan versus the biometric template on the card prior to the generation of the access control transaction. Alternatively, the enrollment scan may be maintained in a local access panel/controller where it could be used for an on-line authentication of the cardholder's identity and access privileges.

4.4 Rostering

The Rostering application allows data residing on the Smart Access Common ID Card to be retrieved, date/time stamped, and transferred to a database that is then used to generate a variety of specialized reports. The Rostering application shall be used not only to retrieve and format data, but also to provide positive proof of attendance. It can be used in the following areas:

- **Meeting Attendance –** Meeting participants are required to insert their cards into a reader as they enter a meeting. Demographic data, such as name, office address, agency, office telephone number, office fax number, and email address are retrieved from the card and uploaded to a database. From this database an attendance listing can be generated;

- **Food Services –** Some agencies provide subsidized food facilities for their employees. Employees are required to insert their card into the reader upon entry into the dining facility. The card is read, providing positive proof of attendance at a meal session. The attendant can view the employee's meal plan privileges, determining from this information whether the employee has a meal plan and has already eaten on the plan, or whether money for the meal should be collected; and

- **Emergency Evacuation –** In fire drills or emergency evacuations, employees are required to insert their cards in readers as they exit a building. Demographic data are retrieved from the card and date/time stamped. Reports can be generated to list which employees have been evacuated from the building. From these reports, missing employees can be identified.

4.4.1 Rostering Functionality

The Rostering application shall provide the following functions:

- **Retrieve Data –** This function shall retrieve specified demographic data stored on the chip;

- **Format Data –** This function shall format data to be uploaded to a specified database;

- **Date /Time Stamp Data –** This function shall affix the date and time the data was read from the card;

- **Upload Data –** This function shall transfer data from the card reader to the specified database; and

- **Generate Rostering Reports –** This function shall generate specific reports. The reports generated shall be dependent on the specific use of the Rostering application.

4.4.2 Rostering Application Data

The data provided by the Rostering application shall be dependent upon the specific use, but shall include at a minimum:

- Name;
- Agency;
- Office address;
- Office telephone number;
- Office fax number;
- E-mail;
- Date/time stamp;
- Location stamp;
- Meal plan (optional for food services application); and

- Other application specific data elements.

4.5 Medical

The Medical application allows basic medical and insurance data to be stored on the card and read, when appropriate, by providers. Additionally, the Medical application can be used to populate claim forms. The following areas shall be covered:

- **Emergency Medical Information** – In emergency situations, basic medical and emergency contact information can be obtained from the card. Such information may include blood type, allergies, next of kin, next of kin phone number, and special medical needs;

- **Insurance Status –** The card provides information about the cardholder's insurance coverage including both primary and secondary health insurers. This data may be used at public or private providers, as well as during the claims submission process; and

- **Claims Submission –** Demographic and insurance data on the card can be retrieved to populate electronic claims submission forms.

4.5.1 Medical Functionality

The Medical application shall provide the following functionality:

- **Input Medical Data –** This function shall allow the user to enter data onto the chip card either through a terminal interface or via a file download from an on-line system (e.g., personnel system). The card reader provides a user interface that shall be used to enter data to be stored on the chip;

- **Update Medical Data –** This function provides the capability for the user to add, modify, or delete Medical data to or from the card;

- **Query/Display Medical Data –**This function provides the capability for the user to request that data be retrieved and displayed on a terminal screen. The user shall be able to specify the conditions for selecting the data to be retrieved or displayed;

- **Print Medical Data –** This function shall provide the capability for the user to specify data to be retrieved, formatted, and printed in hard copy;

- **Maintain Databases –** This function shall provide the capability for the user to specify data to be written to files that can be uploaded to on-line system databases. Transactions shall be able to be collected and uploaded to a central database at the end of the day, or they may be replicated and used to update an on-line database in real-time mode. This capability shall be used to implement either centralized or geographically dispersed back-up files that can be used to restore data to cards issued to replace lost or stolen cards; and

- **Generate Medical Reports –** This function shall generate specific reports. The reports generated shall be dependent on the specific use of the Medical application.

4.5.2 Medical Application Data

The Medical application shall provide the following data:

- Medical needs;
- Next of kin name;
- Next of kin phone;
- Blood type;
- Allergies;
- Religion;
- Primary provider identifier;
- Primary provider name;
- Primary provider address;
- Primary provider phone number;
- Insurance company identifier;
- Primary/secondary indicator;
- Insurance company name;
- Insurance company address;
- Insurance company phone number;
- Insurance policy number;
- Group number;
- Coverage effective date;
- Coverage expiration date;
- Deductibles;
- Required co-payments; and
- Payment priority.

Agencies, at their discretion, may choose to maintain additional medical data on the card. Agencies wishing to use the card for transport and exchange of medical data should adhere to the G-8 Standards for Interoperability between electronic cards that contain health related data that can be associated with specific individuals. By conforming to the G-8 Standards, agencies could achieve interoperability with other health cards.

4.6 Training/Certification

The Training/Certification application allows data about training experiences and job-specific certifications to be entered on the card. Managers can read the card and obtain a view of the employee's training history and licenses/certifications.

4.6.1 Training/Certification Functionality

The Training/Certification application shall provide the following functionality:

- **Input Training/Certification Data –** This function shall allow the user to initially enter data onto the chip card either through a terminal interface or via a file download from an on-line system (e.g., personnel system). The card reader provides a user interface that shall be used to enter data to be stored on the chip;

- **Update Training/Certification Data –**This function shall provide the capability for the user to add, modify, or delete Training/Certification data to or from the card;

- **Query/Display Training/Certification Data –** This function shall provide the capability for the user to request that data be retrieved and displayed on a terminal screen. The user shall be able to specify the conditions for selecting the data to be retrieved or displayed;

- **Print Training/Certification Data –**This function shall provide the capability for the user to specify data to be retrieved, formatted, and printed in hard copy;

- **Maintain Databases** – This function shall provide the capability for the user to specify data to be written to files that can be uploaded to on-line system databases. Transactions shall be able to be collected and uploaded to a central database at the end of the day, or they may be replicated and used to update an on-line database in real-time mode. This capability shall be used to implement either centralized or geographically dispersed back-up files that can be used to restore data to cards issued to replace lost or stolen cards; and

- **Generate Training/Certification Reports –** This function shall generate specific reports. The reports generated shall be dependent on the specific use of the Training/Certification application.

4.6.2 Training/Certificate Application Data

The Training/Certification application shall provide the following data:

- Course identifier;
- Course name;
- Course start date;
- Course end date;
- Course description;
- Course cost;
- Course completion indicator;
- Course grade;
- Hours required;
- Training source identifier;
- Training source name;
- Training source telephone number;
- Certification/license number;
- Certification/license name; and
- Certification/license expiration date.

4.7 Electronic Forms Submission

By combining the use of data maintained on the card with the ability to digitally sign an electronic form, the Smart Access Common ID Card provides the foundation to populate and submit a wide range of standard administrative forms used by virtually all Federal agencies. The Electronic Forms Submission application could be developed and used by employees in multiple agencies to complete, sign, and submit the following forms:

- Personnel transactions (e.g., SF52, Thrift Savings Plan Elections, Bond Elections, etc.);
- Request for Personnel Earnings And Benefit statements;
- Travel requests and vouchers;
- Training requests;
- Medical claims forms; and
- Other administrative forms.

4.7.1 Electronic Forms Functionality

The Electronic Forms Submission application shall provide the following functionality:

- **Select Appropriate Form –** This function shall allow the user to select the form he/she wishes to generate from a menu of available forms;

- **Select and Transfer Data –** This function shall allow the application to automatically select the required data from the appropriate data fields on the chip and transfer them to the terminal or system;

- **Output Data –** This function shall allow the application to take data transferred from the card and input it into the form population application in the required format;

- **Populate Form Data Fields –** This function allows the application to automatically populate the appropriate fields of the specified electronic form;

- **Display Form –**This function shall provide the capability for the user to request display of the populated form on the screen for approval;

- **Edit Form –** This function shall provide the capability for the user to add, modify, or delete data from the displayed form;

- **Digitally Sign Form** - This function shall allow the user to digitally sign the electronic form, certifying that the data is correct and up-to-date. This function shall allow the employee both to generate a digital signature and to retrieve his/her digital certificate from the card; and

- **Submit Form –** This function shall allow the user to electronically submit the digitally signed form and accompanying digital certificate, as well as to indicate the appropriate routing.

4.7.2 Electronic Forms Submission Application Data

The Electronic Forms Submission application shall provide a variety of data depending upon the specific form selected. At a minimum, the application shall provide basic demographic data, in addition to whatever additional information is required by the selected form.

4.8 Financial Applications

While some agencies wish to combine both security and financial applications on the Smart Access Common ID Card, most agencies are opposed to placing financial and security applications on the same card. The combination of financial and security applications raises potential security risks and interoperability issues that must be addressed in such a multi-application environment. Therefore, the following financial applications are likely to be adopted only by a small number of agencies:

- Electronic purse;
- Commercial credit; and
- Commercial debit.

Because card-based financial applications require the participation of financial institutions, those agencies contemplating the combination of financial and security applications on a single card should consider utilizing existing contractual relationships with banks (e.g., GSA Smart Pay Contract). The Department of Treasury has policy authority over financial transactions. Agencies wishing to implement financial transactions on the card platform must obtain prior approval of the Treasury.

Those agencies considering optional financial applications must be concerned with interoperability for financial applications in an open environment. To promote an open system environment and such interoperability, the Smart Access Common ID Card shall comply with the *EMV '96: Integrated Circuit Chip (ICC) Specifications for Payment Systems (Version 3.0).*

4.8.1 Electronic Purse Functionality

The agencies may optionally maintain an Electronic Purse capability on the Smart Access Common ID Card. In providing this functionality, the Smart Access Common ID Card integrated circuit chip shall have the capability to support one or more Electronic Purses, consistent with banking practices. The Electronic Purse application must include capability to revalue the Electronic Purse, track account balances, and settle Electronic Purse transactions.

The Electronic Purse functionality may be required to support a number of applications. It is anticipated that the agencies would use the electronic purse to make low value payments to their employees for the following reasons:

- Payments to replace imprest funds;
- Payments for local travel reimbursements; and
- Payments for transportation subsidies.

The security and processing requirements shall be application specific and are expected to include PIN based and non-PIN transactions and both a contact and contactless interface. Potential applications to be used by the employees may include:

- **Automated Fare Collection –** This application is likely to require a contactless interface and non-PIN based transaction processing;

- **Vending Machine Purchases –** These transactions are low value, usually have a contact interface and are non-PIN based;

- **Retail Purchases –** This application is likely to require a contact interface and PIN based transactions; and

- **Parking Payments –** This application may be contact or contactless and non-PIN based transaction.

The differences in security and transaction processing requirements may result in the need to support multiple purses on a single chip.

The agencies that opt to implement an electronic purse capability on the card must comply with any relevant escheat laws, as well as Regulation E requirements regarding stored value purses.

4.8.1.1 Electronic Purse Functionality

There are currently several viable approaches to implementing Electronic Purses. Some products include the tracking of transactions and the accounting of card balances. Other products do not track individual transactions, but rather treat the electronic money as “cash” once it has been placed on the card. Agencies may adopt whichever approach best supports their internal requirements. Thus, the Electronic Purse application may include the following functionality:

- **Maintain Purse Balance–** This function shall provide the capability to maintain a balance for each electronic purse carried on the card. The purse balance shall be carried on the card and on the central database. The new purse balance shall be written to the card each time a card transaction is processed. This is the actual card balance. A derived card balance shall also be carried on the central database. Each time card transactions are uploaded from the card access and/or revaluing terminals, they shall be posted to the account and a new derived card balance shall be computed. When transactions are posted to a cardholder’s account to derive the new purse balance, the derived card balance shall be compared to the last reported balance carried on the card. Tolerances for the appropriate difference between the derived card balance (carried on the database) and balance carried on the card shall be established. Differences outside the established tolerance, especially when the reported card balance is significantly greater than the derived balance (database), shall be investigated to assess the potential for and prevent fraud;

- **Maintain Purse Status –** This function shall provide the capability to maintain the status of the electronic purse account on the central database. For most cards, the status will be active. An electronic purse that has not been used for a specified period of time will revert to an inactive status. These purse balances shall continue to be maintained on the central database for a specified period of time (the industry standard is about one year from the date of last use). Thereafter, the purse account may be moved off-line but must be returned to the central database and the card status reset to active status if the card is later used. The available balance on all cards must be maintained (on or off-line) to comply with State escheat laws;

- **Maintain Transaction History –** An electronic purse transaction history shall be carried on the central database. This function shall maintain the transaction history, including number of transactions or period of time for which a transaction history shall be maintained in an on-line database;

- **Settle Electronic Purse Transaction –** This function provides the capability to settle electronic purse transactions. Transactions must be settled through the Automated Clearing House (ACH) network or commercial networks; and

- **Replace Card Value –** When a card is lost or stolen, this function provides the capability to transfer to the cardholder’s replacement card funds remaining in a PIN protected electronic purse account. This function also allows transfer of funds remaining in electronic purse accounts without PIN protection to the cardholder’s replacement card after a lock has been put on the card (electronically deactivated) and the remaining balance confirmed.

As indicated above, an individual agency may implement an electronic purse using a “cash” approach. In this type of implementation, transactions would not be tracked, nor balances maintained so that funds residing on a lost card could not be replaced.

4.8.1.2 Electronic Purse Application Data

Depending on the type of implementation, the Electronic Purse application may keep an ongoing purse balance. Optionally, the Electronic Purse application may track the last several transactions including the following data:

- POS terminal identifier;
- Date of transaction; and
- Amount of transaction.

4.8.1.3 Electronic Purse Security

Agencies planning to adopt the optional Electronic Purse application shall adhere to adequate security measures. Adequate security measures shall include:

- Secure mutual authentication of cards and purchase devices;
- Secure mutual authentication of card and card issuer during a funds load transaction;
- Automated and centralized transaction collection;
- Clearing and settlement processes not dependent on intervention by any single person;
- Verification of transaction integrity with automated reporting of suspicious activities (such as electronic purse cards with negative balances or abnormal merchant activities);
- Regular secure upgrading of encryption keys deployed in purchase devices;
- Card and purchase device remote management (for updates or deactivation); and
- Regular security certification of electronic purse components (cards, devices, applications) and their respective providers.

The system must support full auditability (ability to reconcile the funds pool with all transaction logs) and complete accountability (ability to reconstruct a card balance from the transaction logs) to ensure rapid fraud detection as well as proper cardholder service in case of dispute or lost card.

4.8.1.4 Electronic Purse Performance

Agencies wishing to adopt an Electronic Purse application shall require the following performance criteria (some criteria will be applicable only to open purse implementations):

- Transaction speed shall remain under 5 seconds for purchase transactions (one half of one second for balance reader transactions);
- The system shall integrate seamlessly into existing payment infrastructures with automated funds transfer to merchant accounts and accessibility through the existing ATM networks;
- Any cards issued with the acceptance mark of the system shall be useable at any points of service (purchase or load) displaying the acceptance mark across all devices and locations where the service is offered;
- All attended POS devices shall offer automated on-line collection with frequency and time of operation determined by the merchant; and
- The system shall be scaleable without limitation of card count, purchase device count, load device count, issuer and acquirer count and location count.

4.8.2 Commercial Credit/Debit

Some agencies may wish to add to the Smart Access Common ID Card their existing government credit card applications including the following card programs:

- Purchase;
- Travel; and

- Fleet.

The magnetic stripe would be used to access information through an on-line system for these commercial credit applications. Optionally, a commercial debit capability could potentially be added to the card. Both the functionality and data set of the existing magnetic stripe-based capability would be added to the Smart Access Common ID Card.

While GSA does not wish to preclude the option for agencies to combine their existing credit/debit card applications with their employee identification card, it cautions agencies about adding commercial credit or debit applications to the Smart Access Common ID Card before security risk, ownership, liability, and interoperability issues can be resolved. Furthermore, as GSA has existing contractual relationships with financial institutions for these credit and debit applications (as well as for provision of smart cards) through the GSA Smart Pay Contract, it recommends that agencies consider the use of that vehicle for cards requiring commercial financial applications.

5 SECURITY/PRIVACY REQUIREMENTS

5.1 Security Requirements

In addressing the security of an information system that uses the Smart Access Common ID Card both the characteristics of the card itself and the infrastructure which issues, supports, and uses the card shall be considered. According to Section 7.1 of the *Government Smart Card Technical Interoperability Guidelines*: "The Government Smart Card infrastructures may include, but are not limited to, those involved with Government Smart Card design; analysis; fabrication; testing; initialization; distribution; encryption key and digital signature key material generation, distribution, and loading; issuance to cardholder; cardholder data uploading to operational systems and to repositories; cardholder data downloading from repositories to replace damaged or lost cards, audit collection and analysis; commercial system interactions such as point of sale terminals, vending machines, and automatic teller machines; and eventual card replacement, retirement, and disposal."[33] The components of the Smart Access Common ID Card infrastructure shall conform to Section 7 of the *Government Smart Card Technical Interoperability Guidelines*. Additionally, the Department of Defense Smart Card Technology Office Functional Working Group for Security is currently working on a draft security document, entitled *Recommendations for the Secure Implementation of Multiple Applications on Smart Card Devices*, that contains security guidelines for government smart cards. Once this draft is completed, the Smart Access Common ID Card infrastructure shall adhere to these security guidelines. At the time of the publication of this document, security guidelines contained herein are consistent with this draft version. Nevertheless, once finalized, they will be examined for consistency and any revisions incorporated into this document.

For each component of the Smart Access Common ID Card infrastructure and each Smart Access Common ID Card application, an Information System Security Policy (ISSP) shall be generated. The ISSP shall be used in the development of the Smart Access Common ID Card security requirements, evaluation of alternative system design architectures, and assessment of the security effectiveness of the system design, and implementation of the Smart Access Common ID Card applications.

Additionally, the components of the Smart Access Common ID Card infrastructure shall conform to the security recommendations contained in Appendix B of the *Guidelines for Placing Biometrics in Smart Cards*. This Appendix presents information on vulnerabilities of smart card including:

- Physical attacks on the smart card and attacks between the host and the smart card;
- Vulnerabilities of multi-application cards;
- Use of cryptographic algorithms; and
- An overview of token based security mechanisms.

[33] *Government Smart Card Interoperability Guidelines*, Op. Cit., p. 34.

Since the Smart Access Common ID Card is intended to support multiple applications, adequate security provisions shall be in place to allow secure sharing of applications. In an environment in which different "cardlets" (applications running on the smart card) may need to utilize different authentication methods, it is suggested that one cardlet be developed to provide session based authentication methods. According to Appendix B of the *Guidelines for Placing Biometrics in Smart Cards*, the following additional security considerations should be addressed in a multi-application environment:

- A certification method such as FIPS 140-1 certification;
- Signature verification on all downloaded cardlets to prevent unauthorized cardlets from being downloaded to the smart card; and
- Secure file-sharing capabilities.[34]

5.1.1 Card Security

The Smart Access Common ID Card may provide varying functionality at the discretion of individual agencies. The functionality of the card may include:

- Granting read or write access to files;
- Hashing files;
- Calculating digital signatures;
- Verifying digital signatures;
- Providing key exchange; and
- Encrypting data.

The security required for the card may vary, depending on the sensitivity of the data and applications on the card chosen by a particular agency. The Smart Access Common ID Card shall be capable of performing the following functions:

- **Granting File Access –** At a minimum, the Smart Access Common ID Card shall be capable of controlling read and write file access;

- **Hash –** Optionally, the Smart Access Common ID Card may perform a hash function which shall be enabled only after the cardholder has entered a PIN or biometric and the application, which requires the hashing to be performed, has satisfied additional access control requirements; and

- **Digital Signature –** The Smart Access Common ID Card may perform a digital signature function which shall be enabled only after the cardholder has entered a PIN or biometric and the application, which requires the hashing to be performed, has satisfied additional access control requirements.

[34] *Guidelines for Placing Biometrics in Smart Cards*, Op. Cit., p. B-1.

The Smart Access Common ID Card shall implement a graded set of access control security mechanisms and enforce access privileges to card files as specified via these mechanisms. At the discretion of the agency, access control mechanisms may involve a PIN, a password, biometric protection, public key based cryptographic protection, or other approved mechanisms. The operation of the access control mechanisms shall be in conformance with Section 7.3 of the *Government Smart Card Interoperability Guidelines*.[35]

5.1.2 Key Management

If the Smart Access Common ID Card maintains digital signature or encryption keys, these keys shall be maintained in a private file. Access to this file shall be provided only after verifying an entered PIN or biometric scan to authenticate the identity of the cardholder.

5.1.3 Data Security

The Smart Access Common ID Card shall provide for data security in accordance with Section 7.4 of the *Government Smart Card Technical Interoperability Guidelines*.[36] The necessary security services fall into four categories: data origin authentication, confidentiality, integrity, and availability.

5.1.3.1 Authentication

The Smart Access Common ID platform shall provide a mechanism to verify the users identity using at least two of the following components: (1) something that the user has (namely, the Smart Access Common ID Card); (2) something that the user knows (e.g., a password or PIN), and (3) something that the user is (e.g., a biometric measure). The Smart Access Common ID shall be used to digitally store a PIN and/or biometrics measurement that can be required of the smart card user at the time of use.

5.1.3.2 Confidentiality

The Smart Access Common ID platform data shall be protected to ensure that system and confidential information shall not be disclosed for unauthorized purposes. Cardholder privacy shall be ensured in accordance with government and industry standards. Such data security controls shall include the following at a minimum:

- **System Access –** The agency shall ensure that designated users from the agency may only access the system in relation to system data and operations in relation to their specific program applications.

- **Disclosure of Information and Data –** Any sensitive information made available in any format shall be used only for the purpose of carrying out the functions of the Smart Access Common ID Card. Information contained in such material shall not be divulged or made known in any manner to any person except as may be necessary in the performance of the functions authorized by the agency to be performed by the Smart

[35] *Government Smart Card Interoperability Guidelines*, Op. Cit., p. 36-48.
[36] Ibid., p. 48-49.

Access Common ID Platform – Disclosure to anyone other than an authorized officer or employee of the agency is prohibited without prior written approval. Sensitive information shall be accounted for upon receipt and properly stored before, during and after processing. In addition, all related output shall be given the same level of protection as required for the source material.

- **Object Reuse Specifications –** The purpose of object reuse specifications is to prevent the inadvertent disclosure of residual information from data storage devices. When a storage object (including but not limited to, core area and disk file) is initially assigned, allocated, or reallocated to a system user, the system shall assure that it has been cleared.

5.1.3.3 Integrity and Availability

To ensure adequate data integrity and availability, security controls that provide protection from unauthorized access, erasure, tampering and manipulation shall be provided. Such data security controls shall include the following at a minimum:

- **Separation of Duties –** There shall be adequate internal controls through separation of duties and/or dual control for the functions of card and PIN issuance, system administration and security administration (this includes the separation of operations from control functions, such as reconciliation controls);

- **Back-up and Contingency Operations –** There shall be adequate back-up procedures to ensure the continuation of operations in the event of a temporary disruption (i.e., 4 hours or less) in operations;

- **Contingency and Disaster Recovery Plans –** There must be established policies and assigned responsibilities to ensure that appropriate contingency and disaster recovery plans are developed and maintained. Contingency planning consists of the advance plans and arrangements, which are necessary to ensure continuity of the critical functions of the system. A formal Contingency Plan shall be required. The contingency plan shall describe the actions to be taken, the resources to be used and the procedures to be followed before, during, and after any unlikely event occurs that would render inoperative a function supportive to the system. The contingency plan shall cover all events of total or partial cessation of operations or destruction of the database or physical facility. Such planning shall include procedures and availability of equipment for both automated and manual procedures;

- **System and Procedural Documentation –** An integral component of the internal control structure is the provision and maintenance of adequate documentation of system and software applications and operating procedures and requirements;

- **Security Features User's Guide –** A single summary, chapter, or manual in user documentation shall describe the security features provided by the system, guidelines on how to use them, and how they interact with one another; and

- **System Modification and Tampering Controls –** The mechanisms within the application that enforce access controls shall be continuously protected against tampering and/or unauthorized changes. The security-relevant software, or other control mechanisms, shall maintain an execution program that protects its security mechanisms from external interference or tampering (including but not limited to, modification of its code or data structures).

To ensure adequate security, there should be common roles defined by the system to include, but not be limited to:

- Security Officer;
- Auditor;
- Administrator; and
- User.

5.1.4 System Security

The Smart Access Common ID Card shall be a component of an overall system that provides a full range of functionality. The full Smart Access Common ID Card system requires security measures to ensure the secure operation of all components of the system.

This section addresses security and control requirements pertinent to the development and overall operational characteristics of the Smart Access Common ID platform information and processing systems:

- **Control of Card Stock** - There shall be system and procedural controls to ensure that unissued card stock is properly safeguarded against loss, theft, and/or abuse; and

- **Communications Access Controls** - There must be communications software to control access to the Smart Access Common ID platform. Such communications software controls shall ensure that all agency personnel access to the system to input data or generate inquiries is strictly controlled. Communications access control software shall provide for the following capabilities at a minimum:

  - User Identification and Authentication. All personnel requiring access to the system must be established within the system. The system shall require unique identification from each user to access the system (i.e., use ID and password). In addition, the system shall support blind password display. Access to files, databases, transactions and programs shall be restricted to those personnel needing access to such data to meet professional responsibilities. The system shall protect authentication data so that it cannot be accessed by any unauthorized user. The system shall also provide the capability of associating this identity with all actions taken by that individual subject to audit. The system shall be able to maintain information for determining the authorizations of individual users. The system shall support a lock-out threshold for excessive invalid access attempts. The logon IDs and passwords of users no longer authorized to access the system shall be immediately deleted;

- Discretionary Access Controls. The system shall use identification and authorization data to determine user access to information and level or type of information accessed. The system users shall be provided the capability to specify who (by individual user or users, or type of users) may have access to system data. The system or network shall assure that users without that authorization are not allowed access to the data; and

- System Access Audit Controls. The system shall be able to create an audit trail of access to the system and maintain and protect such records from modification, unauthorized access, or destruction. The system shall define and control access between named users and named objects (including but not limited to, files and programs). The system shall be able to record the following types of events: log on, log off, change of password, creation, deletion, opening and closing of files, program initiation, and all actions by system operators, administrators, and security officers. For each recorded event, the audit record shall identify: date and time of the event, user, type of event, and the success or failure of the event. For log on, log off, and password change, the origin of the request (including but not limited to, terminal ID) shall be included in the audit record. For file related events the audit record shall include the file's name. The system administrator (or system security administrator) shall be able to selectively audit the actions of one or more users based on individual identity.

Controls shall be in place to ensure that transaction communications are safeguarded, and transactions are processed only for properly executed transactions from authorized terminals. Communications message validation shall provide for control edits for message completeness, file and field formats, and control and authentication measures. The ability to perform error checking of transmitted data to ensure integrity of transmitted data, including range checks for acceptable data fields and message format checks shall be incorporated into the system. Agencies shall have the ability to employ encryption to ensure message privacy.

5.1.5 Card/System Physical Security

The Smart Access Common ID Card shall provide the following Integrated Circuit Chip and physical card level security protection in accordance with Section 7.5 of the *Government Smart Card Technical Interoperability Guidelines*:[37]

- Tamper deterrent technologies that may prevent tampering with the integrated circuit(s) and information stored on the surface of the card;

[37] Ibid., p. 49-50.

- Tamper resistant technologies that resist tampering with the integrated circuit(s) and information stored on the surface of the card;
- Tamper indicator(s) technologies that indicated tampering with the integrated circuit(s) and information stored on the surface of the card; and
- Authenticator(s) technologies that authenticate the integrated circuit(s) and information stored on the surface of the card.

Additionally, the agency requires physical security and access control systems to limit access to any facilities used to produce cards, process data, or house any sensitive data to those authorized personnel and authorized visitors. The control systems shall have the capability to detect and report attempted unauthorized entries into the facility.

The access to primary and back-up data centers associated with the Smart Access Common ID Card system shall be regulated in such a way that the flow of all persons can be monitored and controlled by a security staff or other control process. This can be accomplished through the utilization of closed circuit television camera systems, card reader access systems, intrusion detection alarm systems or similar systems.

The following minimum physical security protection measures shall be implemented at the card issuer (and related Certificate or Attribute Authorities) to deny unauthorized access to, manipulation, and/or sabotage of the data processing and telecommunications facilities used in the implementation of the Smart Access Common ID system. The following physical controls are needed for the operational facilities of the card issuer, Certificate and/or Attribute Authorities in these areas:

- **Entrance Security –** The data processing and telecommunications facilities shall be secured 24 hours a day, 365 days a year. The entrance(s) to the automated information systems or telecommunications facility shall provide for controlled entry and be secure against forced entry;

- **Locks –** The facility(s) shall be locked at all times when authorized personnel are not present. If undetected entry can occur while the facility is occupied, countermeasures shall be implemented to restrict unauthorized access;

- **Keys –** Keys shall never be left in locks or hidden in an area near the lock. The distribution of keys shall be strictly limited and an effective control system established;

- **Cipher Locks –** Cipher or proximity/swipe card type devices may be used during duty hours to control entry into a facility. However, during non-duty hours, the cipher lock shall not be used as a sole locking device. The cipher combination shall be protected by shielding the user of the locking mechanism against observation by unauthorized personnel and shall be periodically changed;

- **Windows –** Ground level and second story windows shall have positive locking devices installed. If conditions allow, windows should be made inoperable;

- **Personnel Access Controls –** Access to operational sites shall be controlled and limited to authorized personnel. Employee access to controlled areas within the operational site shall be controlled by electronic access or other comparable procedure. Guests, including vendors, shall be required to sign-in and shall be assigned a temporary identification badge, or other comparable control, to be permitted access to the facility. Guests shall be escorted at all times;

- **Data Storage Security –** All data on portable media, including but not limited to, magnetic tapes, diskettes, removable disk packs, paper listings, and microfiche shall be in secure access controlled storage areas with access limited to authorized personnel, when not being used by computer operations; and

- **Fire Protection and Suppression –** The primary and back-up processing sites as well as the tape storage areas shall be equipped with fire detection and suppression systems that detect and suppress fire in the incipient stage.

5.1.6 Application Security

An application requests to retrieve or deposit specific data from or to the Smart Access Common ID Card after authentication of the application, card acceptance device, and Smart Access Common ID Card. The application shall have a secure mechanism (e.g., application security module) to contain and protect its application passwords, algorithms, or keys. The application shall conform to the requirements specified in Section 7.6 of the *Government Smart Card Technical Interoperability Guidelines*.[38] Alternatively, it may be desirable to have most applications utilize a system resource, such as the operating system, to perform user authentication.

5.1.7 Administrative and Personnel Security

The integrity of Smart Access Common ID platform operations including card issuer or Certificate/Attribute Authority personnel involved in system administration and security administration must be ensured. Appropriate screening of all personnel who are assigned to work on the system shall be conducted, and such screening shall be in compliance with Title 12, U.S.C., Section 1829.

To ensure adequate administrative and personnel security for the Smart Access Common ID platform, the following controls shall be in place:

- **General Organizational Controls –** There must be designated organizational entities responsible for security administration. Security and control responsibilities for personnel involved in security administration shall be clearly delineated in the position

[38] Ibid., p. 50-51.

descriptions for such personnel. A Security Program Official shall be designated. This official shall be responsible for the approval of security specifications during the development of the Smart Access Common ID platform. This official shall also be responsible for ensuring that security activities during system development are accomplished and management officials are kept aware of the system security design specifications;

- **Supervisory and Management Controls –** There shall be supervisory and management controls in controlling risks to the system and operation. In addition, there shall be instituted separation of duties, dual control, and/or other measures to control against operational risks;

- **Internal Controls –** Adequate safeguards shall be in place to control against internal theft and/or embezzlement. Such controls shall include pre-employment inquires and National Agency checks on new and temporary personnel; and

- **Security Training –** Security awareness training, in accordance with Public Law 100-235, Computer Security Act of 1987, for all personnel involved in the management, operation, programming, maintenance, or use of the system shall be available. Employees shall be aware of their security responsibilities, know how to fulfill them, and know the penalties involved if they are not fulfilled. Such training shall be directed to the specific system and operational procedures that the personnel shall be using.

All personnel shall be certified as having received the required security awareness training as part of the annual certification described in this section. Additional and refresher training shall be performed annually.

The system security personnel shall receive training in the operations of the system that includes a systemic overview, the security features, known vulnerabilities and threats, and security evaluation methodologies.

5.1.8 Inspections, Audits, and Investigations

The agency shall have the right to inspect, review, investigate, or audit all parts of the facilities engaged in performing services related to the Smart Access Common ID Program. In such capacity, the agency or its representatives shall have access to facilities, records, reports, personnel and other appropriate aspects of the system.

5.1.9 Comprehensive Security Program

A comprehensive security program for the Smart Access Common ID platform and operations shall be required. This program shall include the administrative, physical, technical and systems controls that will be implemented to meet the security requirements of the system and this section. It is the expectation that the system of internal controls used to manage risks to the Smart Access Common ID platform and operations shall be based on industry standards used by system managers to manage their business exposure.

5.2 Privacy Requirements

It is assumed that the data on the Smart Access Common ID Card shall be limited to Sensitive But Unclassified data. While not subject to the regulations protecting classified data, nevertheless, such data shall be subject to privacy protection. Because the Smart Access Common ID Card system will contain individual identifying information, its implementation may require that agencies obtain a Privacy Act clearance.

5.2.1 Legislative Mandate

All applicable Federal privacy laws and regulations shall apply to protecting the data maintained in the Smart Access Common ID Card and system components. Additionally, agency specific regulations that protect the confidentiality of data maintained on the Smart Access Common ID Card and system components shall be adhered to. Such regulations may vary from agency to agency.

5.2.2 Levels of Sensitivity

As the functionality of the Smart Access Common ID Card may vary from agency to agency, there may be corresponding variance in the levels of sensitivity of data and applications on the Smart Access Common ID Card. A mechanism must be in place to address this variance in sensitivity levels. Such a mechanism shall support varying levels of protection for public and confidential data.

5.2.3 Confidentiality Safeguards

The Smart Access Common ID Card platform shall provide a mechanism to designate agency specified confidential data. All cardholder data deemed confidential shall be subject to the safeguards described in Section 5.1.3.2 above.

APPENDIX A – GLOSSARY OF TERMS

Algorithm – A computational procedure used for performing a set of tasks such as an encryption process, a digital signature process, or a cardholder verification.

American Association of Motor Vehicle Administrators (AAMVA) – An association of administrators representing motor vehicle agencies in the United States and Canada.

Anti-tamper – Refers to the technology available to prevent unauthorized alteration or modification of cards.

Anti-tearing – The process or processes that prevent data loss when a smart card is withdrawn from the contracts during a data operation.

Application Program Interface (API) – A formal specification of a collection of procedures and functions available to a client application programmer. These specifications describe the available commands, the arguments (or parameters) that must be provided when calling the command, and the types of return values when the command execution is completed.

Attribute Authority (AA) – An entity responsible for issuing and verifying the validity of an attribute certificate.

Attribute Certificate – A message, similar to a digital certificate, which is intended to convey information about the subject. The attribute certificate is linked to a specific public key certificate. Thus, the attribute certificate conveys a set of attributes along with a public key certificate identifier or entity name.

Authorization – The process of determining what types of activities or access are permitted for a given physical or logical resource. Once the identity of the user has been authenticated, they may be authorized to have access to a specific location, system, or service. In the context of logical access control, the process whereby a user's privileges to access and manipulate data objects are assigned.

Automated Fare Collection – The use of an automated system to collect and process tolls, fares and fees electronically.

Automated Response Unit (ARU) – A designated system for answering telephone calls and providing information to callers via recorded messages, or transferring calls to a customer service center (CSC).

Bar Code – The set of vertical bars of irregular widths representing coded information placed on consumer products and other items (such as identification cards) that may require this type of identification.

Binding – An affirmation by a Certificate Authority/Attribute Authority (or its acting Registration Authority) of the relationship between a named entity and its public key or biometric template.

Biometric Template – Refers to a stored record of an individual's biometric features. Typically, a "livescan" of an individual's biometric attributes is translated through a specific algorithm into a digital record that can be stored in a database or on an integrated circuit chip card. The formatted digital record used to store the biometric attributes is generally referred to as the biometric template.

Biometrics – An automatic identification process for identity verification of individuals based on unique behavioral or physiological characteristics. These are unique things that we do or unique physical characteristics that we have. Behavioral biometrics include voice, signature, and keyboard typing technique. Physical biometrics include fingerprint, hand geometry, facial recognition, and iris and retinal scan.

Bridge Certificate Authority – An entity that links two or more Certification Authorities who do not have a cross-certification agreement in place. The Bridge Certificate Authority allows CAs to validate each other's certificates.

Card Accepting Device – A device that is used to communicate with the Integrated Circuit Card (ICC) during a transaction. It may also provide power and timing to the ICC.

Card Hot List – A list of cards that have been reported as lost, stolen or damaged.

Card Initialization – Refers to the process of preparing a card for use by performing the following tasks: searching for initialization files, locating definite values to use in place of variable values, and loading these values.

Card Personalization – Refers to the modification of a card such that it contains data specific to the cardholder. Methods of personalization may include encoding the magnetic stripe or bar code, loading data on the ICC, or printing photo or signature data on the card.

Card Printer – Equipment capable of printing information on the physical surface of the card.

Card Reader – Equipment capable of reading the information on a card such as that in the magnetic stripe or chip.

Cardholder – The person or entity to whom a card is issued.

Certificate Authority (CA) – The Certificate Authority is a component of the Public Key Infrastructure. The CA is responsible for issuing and verifying digital certificates. Digital certificates may contain the public key or information pertinent to the public key.

Certificate Arbitrator Module – (CAM) – A system that interfaces with agency applications that receives a request for the status of a certificate, passes the certificate validation request to the appropriate CA, receives the certificate validation request response, returned from the CA, and reports the response to the requesting agency application.

Certificate Policy – A document that sets forth the rules established by the policy issuing entity governing the issuance, maintenance, use, reliance upon, and revocation of digital certificates.

Certificate Repository – A database of certificates and other PKI relevant information available on-line.

Certificate Revocation List (CRL) – A periodically issued list, digitally signed by a CA, of identified certificates that have been suspended or revoked prior to their expiration dates. The list generally indicates the CRL issuer's name, the date of issue, the date of the next scheduled CRL issue, the suspended or revoked certificates' serial numbers, and the specific times and reasons for suspension and revocation.

Certification Practice Statement (CPS) – A document that states the practices that a Certificate Authority employs in issuing certificates.

Chip – A small piece of thin semiconductor material, such as silicon, that has been chemically processed to have a specific set of electrical characteristics such as circuits, storage, or logic elements. Also known as Integrated Circuit (IC)

Chip Card – A card into which one or more integrated circuits is inserted. Includes both microprocessor cards and memory cards.

Chip (Card) Operating System (COS) – The operating system within a card's integrated circuit that interprets commands sent by the workstation and performs the functions requested.

Clearance –A designation of an authorized security level granted by a governmental authority to an individual that allows the individual to have access to physical locations, documents, or information that has the corresponding security level associated with the clearance level.

Compromise – A violation (or suspected violation) of a security policy, in which an unauthorized disclosure of, or loss of control over, sensitive information may have occurred.

Contact Interface – A chip card that allows interface through a contact. A contact is an electrical connecting surface on an ICC and/or interfacing device that permits a flow of energy current, thereby transmission of data.

Contactless Interface – An ICC that enables energy to flow between the card and the interfacing device without the use of contact. Instead, induction of high-frequency transmission techniques are used through a radio frequency (RF) interface.

Cryptographic Co-Processor – An integrated circuit chip processor that performs cryptographic functions.

Cryptography – The mathematical science used to secure the confidentiality and authentication of data by replacing it with a transformed version that can be reconverted to reveal the original data only by someone holding the proper cryptographic algorithm and key.

Customer Service Center (CSC) – A customer service unit staffed with operators or customer service representatives (CSRs). Customer service representatives are responsible for taking telephone calls and providing information and services to clients as needed.

Data Integrity – A condition in which data has not been altered or destroyed in an unauthorized manner.

Debit Card – A card that can be used to make purchases or obtain cash advances at designated retail locations or automated teller machines. The cardholder's account is debited when a purchase or cash advance is made.

Digital Certificate – A portable block of data, in a standardized format, which at least identifies the certificate authority issuing it, names or identifies its subscriber, contains the subscriber's public key, identifies its operational period, and is digitally signed by the certificate authority issuing it.

Digital Signature – A unique electronic signature that accompanies documents and messages. The digital signature serves two primary functions: verifies the authenticity of the party sending the message, and verifies that the content of the message has not been altered.

Digitized Signature – A written signature that has been read by a computer scanner and converted into digital data.

Distinguished Name – A set of data that identifies a real-world entity, such as a person in a computer-based context.

Electronic Purse – A mechanism that allows end users to pay electronically for goods and services. The function of the electronic purse is to maintain a pool of value that is decremented as transactions are performed.

Encryption – Refers to the process of translating data into a cipher, a more secure form of data. Encrypted data is less likely to be intercepted and accessed by unauthorized persons. This mechanism is particularly important in executing sensitive transactions.

Enrollment Station – A designated workstation which is used to collect data to enroll individuals for the Smart Access Common ID Card.

Extensions – Extension fields in X.509 Version 3 certificates.

False Acceptance Rate (FAR) – Refers to the rate at which an unauthorized individual is accepted by the system as a valid user.

False Rejection Rate (FRR) – Refers to the rate at which an individual authorized to use the system is rejected as an invalid user.

Graphical User Interface (GUI) – A user interface to a computer that is graphics-based, rather than textual or command-based.

Hashing – A software process which computes a value (hashword) from a particular data unit in a manner that enables detection of intentional/unauthorized or unintentional/accidental data modification by the recipient of the data.

Identification Authentication – The process of determining the identity of a user that is attempting to access a physical location or computer resource. Authentication can occur through a variety of mechanisms including challenge/response, time-based code sequences, biometric comparison, or other techniques.

Integrated Circuit Chip Card – A card containing a microprocessor and memory capable of making decisions and processing data.

International Standards Organization (ISO) – A worldwide organization dedicated to fostering the development of systems standards. National standards organizations from 100 different countries are members of the ISO, including the United States (American National Standards Institute – ANSI). Member organizations participate in the development of ISO standards.

Interoperability – Refers to a system or a product that is capable of operating with another system or product directly, (i.e. without any additional effort from the user). Interoperability can be achieved through mutual conformance to a set of common standards and specifications. Interoperability may also be achieved through the use of a “service broker” able to convert one interface into another interface directly.

Key – A value that particularizes the use of a cryptographic system.

Key Management – The process and means by which keys are generated, stored, protected, transferred, loaded, used, revoked, published, and destroyed.

Key Pair – The key pair consists of a private key and its matching public key.

Lightweight Directory Access Protocol (LDAP)– LDAP is an emerging software protocol for enabling anyone to locate organizations, individuals, and other resources such as files and devices in a network, whether on the Internet or on a corporate intranet. LDAP is a "lightweight" (smaller amount of code) version of DAP (Directory Access Protocol), which is part of X.500, a standard for directory services in a network.

Logical Access Control – An automated system that controls an individual's ability to access one or more computer system resources such as a workstation, network, application, or database. A logical access control system requires validation of an individual's identity through some mechanism such as a PIN, card, biometric, or other token. It has the capability to assign different access privileges to different persons depending on their roles and responsibilities in an organization.

Local Access Panel/Controller (LAP/C) – Refers to a device used to monitor and control access to a site by utilizing an intelligent local processing capability in combination with downloaded database processing.

Mandatory – Indicates a service or function that must be provided by the vendor team, or a requirement or condition that must be met without exception. For the purposes of this document, Vendors must provide products and services to address all mandatory requirements. The term mandatory refers only to the Vendor's obligation to meet these requirements, and does not imply that agencies will choose these products and services. Agencies are *not required* to utilize mandatory products, services, or capabilities.

Mean Time Between Failures (MTBF) – The estimated length of time that a system is available and operational between failures.

Mean Time To Repair (MTTR) – The estimated length of time needed to bring a system back up and make it fully operational following a system failure.

Nonrepudiation – Refers to the determination that data was sent by one party and received by another party, and can be verified by the inclusion of information about the origin or delivery of the data. Nonrepudiation protects both the sender and the recipient of data from false claims that the data was either not sent, or not received.

Open Database Connectivity (ODBC) – Refers to an open or standard application programming interface (API) used to access a database. A database that is ODBC-compliant facilitates the importing, exporting and converting of files from external databases.

Open Systems Environment – A comprehensive set of interfaces, services, and supporting formats, plus user aspects for interoperability or for portability of applications, data, or people, as specified by information technology standards and profiles. An open platform is composed of hardware and software components that adhere to common standards and are non-proprietary such that multiple vendors can supply these components interchangeably. In an open platform, components from multiple vendors using different technological approaches may be assembled and interoperability across products can be ensured. The objective of an open platform is to achieve vendor independence and allow easy transition to emerging technologies.

Optional – For the purposes of this document, the term optional indicates a service or function that is not part of the mandatory requirements, but may be an agency-specific requirement. These functions and services may be provided at the discretion of the vendor team. Agencies are not obligated to procure these services from the vendor team.

Password – Confidential authentication information, usually composed of a string of characters used to provide access to a computer resource.

Personal Identification Number (PIN) – A private series of numbers that a user knows that are used to increase confidence in a user's professed identity.

Physical Access Control – Refers to an automated system that controls an individual's ability to access to a physical location such as a building, parking lot, office, or other designated physical space. A physical access control system requires validation of an individual's identity through some mechanism such as a PIN, card, biometric, or other token prior to providing access. It has the capability to assign different access privileges to different persons depending on their roles and responsibilities in an organization.

Point of Sale (POS) – Generally refers to a site where purchases are made. For the purposes of this document, POS refers to a site where purchases may be made electronically through an electronic cash register or card acceptance device.

Primary Account Number (PAN) – A unique identifying number used to reference a financial account.

Private Key – A mathematical key (kept secret by the holder) used to create digital signatures, and, depending upon the algorithm, to decrypt messages or files encrypted (for confidentiality) with the corresponding public key.

Proximity – Refers to a technology used to provide physical access control. This technology uses a contactless interface with a card reader. An antenna is embedded in the card, which emits a unique radio frequency when in close proximity to the electronic field of the card reader.

Public (Asymmetric) Key Cryptography – A type of cryptography that uses a key pair of mathematically related cryptographic keys. The public key can be made available to anyone who wishes to use it and can encrypt information or verify a digital signature; the private key is kept secret by its holder and can decrypt information or generate a digital signature.

Public Key Infrastructure (PKI) – The architecture, organization, techniques, practices, and procedures that collectively support the implementation and operation of a certificate-based public key cryptographic system. Further, a communications infrastructure that allows users to exchange money and data over the Internet in a secure environment. There are four basic components to the PKI: the certificate authority (CA) responsible for issuing and verifying digital certificates, the registration authority (RA) which provides verification to the CA prior to issuance of digital certificates, one or multiple directories to hold certificates (with public keys), and a system for managing the certificates. Included also in a PKI are the certificate policies and agreements among parties that document the operating rules, procedural policies, and liabilities of the parties operating within the PKI.

Public Key – A mathematical key that can be made publicly available and which is used to verify signatures created with its corresponding private key. Depending on the algorithm, public keys are also used to encrypt messages or files which can then be decrypted with the corresponding private key.

Radio Frequency Identification (RFID) – Refers to an access control system that features a tag embedded with both a circuit and an antenna. As the antenna enters the electronic field of the reader, it generates energy for the circuit, and transmits the identification number in the tag to the reader.

Registration Authority (RA) – The Registration Authority is a component of the Public Key Infrastructure. The RA acts as a gatekeeper by providing verification to the Certificate Authority before granting a request for a digital certificate.

Relying Party – A recipient who acts in reliance on a certificate and digital signature.

Renewal – The process of obtaining a new certificate of the same class and type for the same subject once an existing certificate has expired.

Revocation – The process of permanently ending the operational period of a certificate from a specified time forward. Generally, revocation is performed when a private key has been compromised.

Root – The CA that issues the first certificate in a certification chain. The root's public key must be known in advance by a certificate user in order to validate a certificate chain.

Secret (Symmetric) Key Cryptography – A cryptographic system that uses the same key, known as a "secret key algorithm" to encipher and decipher messages. This is contrasted with asymmetric key cryptography, which uses a secure public/private key pair.

Secure Access Module (SAM) – A software module contained in a card access device that allows the card and terminal to mutually authenticate each other.

Security –Features and procedures used to reduce the possibility of fraudulent use, asset compromise, smart card counterfeiting, or other subversion.

Security Policy – A document that articulates requirements and good practices regarding the protections maintained by a trustworthy system.

Sensitive Compartmentalized Information Facility (SCIF) –A designated physical location that requires high-level security clearance for entry. An area that is generally used to maintain top secret documents and systems.

Speaker Identity Verification (SIV) – The key feature of voice recognition software that extracts and compares unique features of a speech sample with a known sample, and accepts or rejects access based on this comparison.

Storage – An electronic and/or mechanical-magnetic device that holds information for subsequent use or retrieval.

Subscriber – A person who is the subject of, has been issued a certificate, and is capable of using, and authorized to use, the private key that corresponds to the public key listed in the certificate.

Tampering – Refers to any unauthorized alteration or modification of a card.

Token – A hardware security token containing a user’s private key(s), public key certificate, and optionally other certificates.

Wiegand – Refers to a technology that provides physical access control capability by way of a contact interface that is “swiped” similar to a magnetic stripe card. A Wiegand card is more secure and durable than a magnetic stripe card because it is embedded with a magnetic coating during production.

APPENDIX B - RECOMMENDED X.509 CERTIFICATE FORMAT*

Required Certificate Fields

Object/Attribute	Type	Requirement	Comment
Basic Certificate			
Version	INTEGER	SMART ACCESS COMMON ID should require v3 or later; i.e., version=2.	0 = v1, 1 = v2, 2 = v3.
SerialNumber	INTEGER	SerialNumber should be unique for each certificate issued by a given SMART ACCESS COMMON ID contractor.	
Signature	SEQUENCE	Note that the "parameters" field should not be used.	Information re: the Issuer's (SMART ACCESS COMMON ID contractor's) signature.
AlgorithmIdentifier	AlgorithmIdentifier		
Issuer	SEQUENCE of RelativeDistinguishedName		Reference for Distinguished Name: ITU-T Recommendation X.501 | ISO/IEC 9594-2:1997, *Information Technology – Open Systems Interconnection – The Directory: Models*, 1997.
Validity	SEQUENCE		
NotBefore	Time	Time fields should use Coordinated Universal Time as the reference time base. Time should be synchronized within one second of the Master Clock at the U.S. Naval Observatory. The Distinguished Encoding Rules (DERs) allow several methods for formatting time. To ensure that "time" fields are consistently formatted, SMART ACCESS COMMON ID certificates should follow the Federal PKI Working Group recommendation *(Federal PKI Version 1 Technical Specifications: Part E – X.509 Certificate and CRL Extensions Profile)* that all "UTCTime" fields that are encoded using DERs in the "Z" format and must never omit the "seconds" field (even when it is "00") (i.e., the format should be YYMMDDHHMMSSZ). Further, the system should interpret the year field, YY, as 19YY when YY is greater than or equal to 50, and 20YY when YY is less than 50.	ITU-T Recommendation X.690, *Information Technology – ASN.1 Encoding Rules – Specification of Basic Encoding Rules, Canonical Encoding Rules and Distinguished Encoding Rules*, 1994.

Object/Attribute	Type	Requirement	Comment
NotAfter	Time	See above cell.	
Subject	SEQUENCE of RelativeDistinguishedName		Reference for subject: ITU-T Recommendation X.500 | ISO/IEC 9594-1:1997, *Information Technology – Open Systems Interconnection – The Directory: Overview of Concepts, Models, and Services*, 1997. Reference for Distinguished Name: ITU-T Recommendation X.501 | ISO/IEC 9594-2:1997, *Information Technology – Open Systems Interconnection – The Directory: Models*, 1997. Reference for CommonName: ITU-T Rec. X.521 | ISO/IEC 9594-6:1994, *Information technology – Open Systems Interconnection –The Directory: Selected Object Classes*, 1994.
Organization	Directory String	Every SMART ACCESS COMMON ID Business Representative Subscriber certificate should contain an Organization field wherein O=the name of the business. Every SMART ACCESS COMMON ID Agency Application Subscriber certificate should contain an Organization field wherein O=U.S. Government.	
OrganizationalUnit	DirectoryString	Every SMART ACCESS COMMON ID Agency Application certificate should contain an OrganizationalUnit field wherein OU=as listed in the AB Codelist.	

Object/Attribute	Type	Requirement	Comment
Person	CommonName		
CommonName	DirectoryString	Every SMART ACCESS COMMON ID Individual Subscriber certificate should contain the CommonName field wherein CN=name of applicant. Every SMART ACCESS COMMON ID Business Representative Subscriber certificate should contain a CommonName field wherein CN=the name of the applicant. Every SMART ACCESS COMMON ID Agency Application certificate should contain CN, the CommonName field wherein CN=the name of the agency application.	A common name is not a directory name; it is an attribute of the object person; ex: CN=John Doe.
SubjectPublicKeyInfo	SEQUENCE		
Algorithm	AlgorithmIdentifier		
AlgorithmIdentifier			
Parameters			Note that the use of the “parameters” field is allowed, but not required, in subject PublicKeyInfo (depending upon algorithmIdentifier).
SubjectPublicKey	BIT STRING		
SubjectUniqueIdentifier	UniqueIdentifier	Note that this field is required in all SMART ACCESS COMMON ID certificates; it should contain **TBD** (to be determined).	
Extensions			
KeyUsage	EXTENSION	The “critical” Boolean should be TRUE.	“Critical” indicates that any using system that does not recognize this field type or does not implement the semantics of the extension should consider the certificate invalid.
KeyUsage	BIT STRING	The “”digitalSignature” bit should be set to “1,” the “nonRepudiation” bit should be set to “1,” and all other bits should be set to “0”.	This setting indicates key is used for digital signature (e.g., ephemeral authentication) and non-repudiation only.

Object/Attribute	Type	Requirement	Comment
basicConstraints	EXTENSION	The basicConstraints extension should be required in all SMART ACCESS COMMON ID certificates, marked as "critical" (i.e., criticality flag set to "true"), and set to indicate that, aside from SMART ACCESS COMMON ID Contractors, no other SMART ACCESS COMMON ID subscribers are trusted to issue SMART ACCESS COMMON ID certificates.	That is, SMART ACCESS COMMON ID Contractor certificates should have the CA Boolean set to "true," and all other SMART ACCESS COMMON ID certificates should have the CA Boolean set to "false.".
CertificatePolicies	EXTENSION	The "critical" Boolean should be FALSE.	"Critical" indicates that any using system that does not recognize this field type or does not implement the semantics of the extension should consider the certificate invalid.
CertPolicyId	ObjectIdentifier	SMART ACCESS COMMON ID CertPolicyId OIDs should be **TBD.**	OBJECT IDENTIFIER's for SMART ACCESS COMMON ID policy for 1) Individual Subscriber and 2) Business and Agency Application Subscriber certificates will be assigned in near future by the Computer Security Objects Register at the National Institute of Standards and Technology.
Signed Macro			
Signature	SIGNED SEQUENCE	Note that the "parameters" field should not be used.	Issuer's signature, applied over all certificate fields.
AlgorithmIdentifier	AlgorithmIdentifier		
ENCRYPTED-HASH	BIT STRING		

*This chart adapted from: U.S. General Services Administration, Federal Telecommunications Service, Office of Information Security, *Access Certificates for Electronic Services (ACES) Request for Proposals(RFP) Multiple Award Schedule (MAS) Solicitation Number TIBA98003A*, January 4, 1999.

APPENDIX C – LISTING OF AGENCY PARTICIPANTS

The requirements contained in this document are based on information gathered through interviews conducted with a broad range of Federal agencies. The Smart Access Common ID Card Project Team acknowledges the input of the following agency representatives:

Name	**Agency**
Diane Allison	Department of Justice
Peter Alterman	National Institute of Health
Gary Bockwag	US Courts
Tom Boswell	Department of Education
John Brinkema	US Courts
Tom Buckle	Department of Energy
Sue Campbell	Social Security Administration
Thomas Dale Carter	US Marshall Service
Ken Combs	Department of Health and Human Services
Bruce Davis	US Postal Service
Peggy Dodd	Department of Health and Human Services
Frank Dozier	US Courts
Clarence Edwards	General Services Administration
Ed Forest	Department of Navy
Paul Grant	General Services Administration/Dept. of Defense
Richard Guida	US Treasury
Steve Hanson	United States Patent Office
Janis Heiath	Department of Defense
Roberta Heintz	Department of Interior
Richard Hipkins	Department of Interior
Don Heffernan	General Services Administration
Daryl Hendricks	General Services Administration
Mr. Hubbach	USAID
Dean Hunter	General Services Administration
Wilson Innes	Department of Navy
John Jacob	Department of Transportation
Jeff Johns	Department of Transportation
Pete Myo Khin	US Postal Service
Robert Lewis	Environmental Protection Agency
Paul Ma	NASA
Dan Maloney	Department of Veterans Affairs
Dave Mathews	Department of Interior
Michelle Moldenhauer	Treasury
Ed McGuire	Department of Commerce
Bob McMenimen	Department of Treasury
Carl Petransky	Department of Energy
Sherrie Phelps	General Services Administration
Susan Polinsky	Department of Treasury

Name	**Agency**
John Sabo	Social Security Administration
Mike Seely	Department of Commerce
Bradley Smith	Department of Energy –
Judy Spencer	General Services Administration
Borris Stan	Department of Energy
Lt. Col. Steve Tamarind	Department of Navy
David Tippets	Treasury IRS
Gerald Toms	Department of Energy
Tim Vitgotsky	Department of Interior
Bradley Wood	Department of Energy
George Zinkgraf	US Postal Inspections

APPENDIX D – EXISTING GSA GOVERNMENT SMART CARD APPLICATIONS

GSA FTS/Citibank Multi-Application Pilot

- Travel
- Building Access
- Small Purchase
- Personal Property
- Phone Card
- Boarding Pass
- Digital Signature

GSA/Navy Technology Center

- Access Control
- Biometrics
- Navy-Medical/Dental
- E-Purse
- Vendor Displays
- Kiosk Transaction
- Man Overboard